# BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of The original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

## IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
Please do not report the images to the
Image Problem Mailbox.**

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－327147

(43)公開日　平成10年(1998)12月８日

| (51)Int.Cl.[6] | | 識別記号 | FI | | |
|---|---|---|---|---|---|
| Ｈ０４Ｌ | 9/32 | | Ｈ０４Ｌ | 9/00 | ６７５Ｄ |
| Ｇ０９Ｃ | 1/00 | ６４０ | Ｇ０９Ｃ | 1/00 | ６４０Ｂ |
| | | ６６０ | | | ６６０Ｂ |
| | | | | | ６６０Ａ |
| Ｈ０４Ｌ | 9/10 | | Ｈ０４Ｌ | 9/00 | ６２１Ｚ |

審査請求　未請求　請求項の数30　ＦＤ　（全 54 頁）

(21)出願番号　特願平9－147319

(22)出願日　平成９年(1997)５月21日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　洲崎　誠一
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(72)発明者　水野　康彦
神奈川県川崎市幸区鹿島田890番地　株式会社日立製作所ビジネスシステム開発センタ内

(74)代理人　弁理士　矢島　保夫

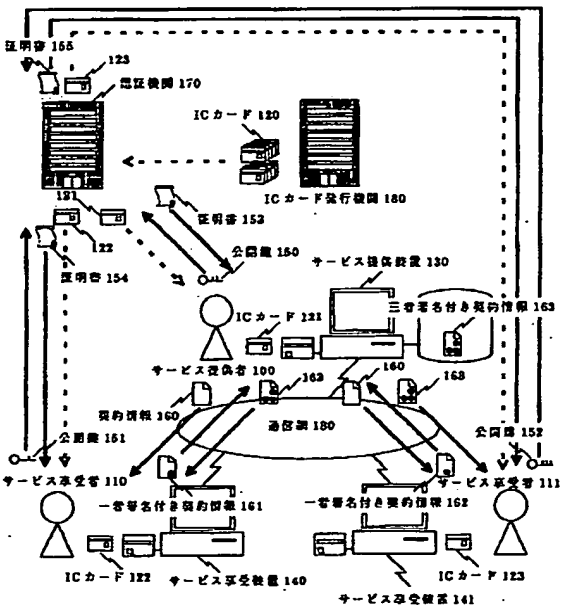
最終頁に続く

(54)【発明の名称】　電子認証公証方法およびシステム

(57)【要約】　（修正有）

【課題】オープンなネットワーク環境において電子商取引に必要な認証・公証サービスを実現する。

【解決手段】サービス提供装置１３０から契約内容を含む契約情報を契約者である各サービス享受者１１０，１１１のサービス享受装置１４０，１４１に送信し、契約情報を受信した各サービス享受装置で契約情報にサービス享受者の署名を付けた一者署名付き契約情報１６１，１６２を作成してサービス提供装置に送信する。サービス提供装置では各サービス享受装置から送信された一者署名付き契約情報を受信し、まとめて一つの文書にし、サービス提供者の署名を付けたサービス提供者署名付き契約情報１６３を作成し、保管するとともに各サービス享受装置に送信する。



1

【特許請求の範囲】

【請求項１】公証サービスを提供するサービス提供者が使用するサービス提供装置と、公証サービスを享受する複数のサービス享受者がそれぞれ使用する複数のサービス享受装置とが、ネットワークを介して相互に接続されているシステムに適用する電子認証公証方法であって、

前記サービス提供装置から、契約内容を含む契約情報を、契約者である各サービス享受者のサービス享受装置に、それぞれ送信するステップと、

該契約情報を受信した各サービス享受装置で、該契約情報にサービス享受者の署名を付けた一者署名付き契約情報を作成し、前記サービス提供装置に送信するステップと、

前記サービス提供装置で、前記各サービス享受装置からそれぞれ送信された一者署名付き契約情報を受信し、受信した複数の一者署名付き契約情報をまとめて一つの文書にするとともに、該文書にサービス提供者の署名を付けたサービス提供者署名付き契約情報を作成するステップと、

前記サービス提供装置で、作成したサービス提供者署名付き契約情報を保管するステップと、

前記サービス提供者署名付き契約情報を、前記サービス提供装置から前記各サービス享受装置に送信するステップとを備えたことを特徴とする電子認証公証方法。

【請求項２】公証サービスを提供するサービス提供者が使用するサービス提供装置と、公証サービスを享受する複数のサービス享受者が使用する複数のサービス享受装置と、前記サービス提供者および各サービス享受者の公開鍵が確かにその者の公開鍵であることを保証する証明書を発行する認証機関の端末装置とが、ネットワークを介して相互に接続されているシステムに適用する電子認証公証方法であって、

前記サービス提供装置で、前記サービス提供者の公開鍵と秘密鍵とを生成するステップと、

前記各サービス享受装置で、それぞれ、前記各サービス享受者の公開鍵と秘密鍵とを生成するステップと、

前記サービス提供装置および各サービス享受装置から、生成した公開鍵を前記認証機関の端末装置に送信するステップと、

前記認証機関の端末装置で、受信した公開鍵ごとに、その公開鍵に対応する証明書を作成し、それぞれ対応する前記サービス提供装置および各サービス享受装置に送信するステップと、

前記サービス提供装置および各サービス享受装置で、前記証明書をそれぞれ受信するステップと、

前記各サービス享受装置から、それぞれ、契約内容その他の契約に係る各種の情報を前記サービス提供装置に送信するステップと、

前記サービス提供装置において、前記各サービス享受装置からそれぞれ送られてくる契約に係る各種の情報をまとめて契約内容を含む契約情報を作成し、前記各サービス享受装置にそれぞれ送信するステップと、

前記各サービス享受装置で、それぞれ、受信した契約情報にサービス享受者の証明書を含む付属情報を所定の順序で連結したデータを作成し、該連結したデータを所定の一方向性関数で圧縮した圧縮子を生成し、該圧縮子をサービス享受者の秘密鍵で暗号化した署名を生成し、前記連結したデータに該署名を合わせて一者署名付き契約情報を作成し、該一者署名付き契約情報を前記サービス提供装置に送信するステップと、

前記サービス提供装置で、前記各サービス享受装置からそれぞれ送信された一者署名付き契約情報を受信し、受信した複数の一者署名付き契約情報から契約情報並びに各サービス享受者が付加した付属情報および署名を取り出し、取り出した情報とサービス提供者の証明書を含む付属情報とを所定の順序で連結したデータを作成し、該連結したデータを所定の一方向性関数で圧縮した圧縮子を生成し、該圧縮子をサービス提供者の秘密鍵で暗号化した署名を生成し、前記連結したデータに該署名を合わせてサービス提供者署名付き契約情報を作成するステップと、

前記サービス提供装置で、作成したサービス提供者署名付き契約情報を保管するステップと、

前記サービス提供者署名付き契約情報を、前記サービス提供装置から前記各サービス享受装置に送信するステップとを備えたことを特徴とする電子認証公証方法。

【請求項３】前記ネットワークを介したサービス提供者およびサービス享受者と認証機関との間の通信は、認証機関の公開鍵と公開鍵暗号とを使用して鍵交換を行ない、その交換した鍵と共通鍵暗号とを使用した暗号通信により行なう請求項２に記載の電子認証公証方法。

【請求項４】前記ネットワークを介したサービス提供者とサービス享受者との間の通信は、互いの証明書を交換し、サービス提供者の公開鍵と公開鍵暗号とを使用して鍵交換を行ない、その交換した鍵と共通鍵暗号とを使用した暗号通信により行なう請求項１または２の何れか１つに記載の電子認証公証方法。

【請求項５】前記サービス提供者および各サービス享受者には、前記認証機関の公開鍵である認証機関証明書が格納されている、前記サービス提供装置およびサービス享受装置に着脱可能な、記憶媒体が、あらかじめ配布されており、

前記サービス提供者および各サービス享受者の公開鍵および秘密鍵、並びに、前記認証機関が発行した証明書は、該記憶媒体に格納される請求項１または２の何れか１つに記載の電子認証公証方法。

【請求項６】前記着脱可能な記憶媒体が、秘密鍵と公開鍵を生成する暗号鍵生成プログラムおよび入力したデータを秘密鍵で暗号化して署名を生成し出力するディジタル署名生成プログラム、並びにそれらのプログラムを実

行して暗号鍵生成や署名生成を実行する処理装置を備えたＩＣカードであり、
前記サービス提供者および各サービス享受者は、該ＩＣカードを用いて、秘密鍵と公開鍵の生成、および署名の生成を行なうとともに、生成した秘密鍵と公開鍵および前記認証機関から送付された証明書は該ＩＣカードに格納する請求項５に記載の電子認証公証方法。
【請求項７】前記着脱可能な記憶媒体には、当該記憶媒体の正当な使用者のパスワードで暗号化された暗号化秘密鍵、暗号化公開鍵、および暗号化自証明書、並びに該パスワードをチェックするためのパスワードチェック用データが格納され、上記暗号化秘密鍵、暗号化公開鍵、および暗号化自証明書にアクセスする際には、使用者が入力したパスワードを上記パスワードチェック用データを用いてチェックし、正当な使用者であると確認された場合のみアクセスを許可する請求項５に記載の電子認証公証方法。
【請求項８】前記着脱可能な記憶媒体が、内蔵時計、秘密鍵と公開鍵を生成する暗号鍵生成プログラムおよび入力したデータを秘密鍵で暗号化して署名を生成し出力するディジタル署名生成プログラム、並びにそれらのプログラムを実行して暗号鍵生成や署名生成を実行する処理装置を備えたＩＣカードであり、
前記サービス提供者および各サービス享受者は、該ＩＣカードを用いて、秘密鍵と公開鍵の生成および署名の生成を行なうとともに、生成した秘密鍵と公開鍵および前記認証機関から送付された証明書は該ＩＣカードに格納し、署名生成時には署名対象のデータに上記内蔵時計の日時データを付加したデータを秘密鍵で暗号化して署名生成する請求項５に記載の電子認証公証方法。
【請求項９】前記ＩＣカードは、署名生成の直前に、時刻管理機関が送信する正確な時刻を示す標準時刻データを受信し、該標準時刻データに基づいて内蔵時計を調整する請求項８に記載の電子認証公証方法。
【請求項１０】前記ＩＣカードは無線受信装置を備え、該無線受信装置により受信した前記時刻管理機関からの標準時刻データに基づいて内蔵時計を調整する請求項９に記載の電子認証公証方法。
【請求項１１】前記着脱可能な記憶媒体内の秘密鍵、公開鍵、および証明書を用いて署名を行なったとき署名履歴を該記憶媒体内に記憶しておくとともに、該記憶媒体内の秘密鍵、公開鍵、および証明書が新たなデータに変更されたとき、署名履歴を参照して必要があれば、以前に使用した秘密鍵、公開鍵、および証明書を別領域に記憶しておく請求項５に記載の電子認証公証方法。
【請求項１２】会員認証局の端末と、個人認証局の端末と、申込者の端末とが、ネットワークを介して相互に接続されているシステムに適用する電子認証方法であって、
あらかじめ、各申込者が、その申込者の公開鍵とその公開鍵がその申込者のものであることを証明する証明書とを含むディジタルデータである個人認証書の配布を前記個人認証局から受けるステップと、
前記申込者の端末から前記会員認証局の端末に、個人認証書を添付した会員登録申込書を送信するステップと、
前記会員認証局の端末から前記個人認証局の端末に、受信した個人認証書の有効性の確認依頼を送信するステップと、
前記個人認証局の端末で、受信した個人認証書の有効性を確認し、確認結果を前記会員認証局の端末に送信するステップと、
前記会員認証局の端末で、その確認結果に基づいて前記申込者の会員資格の審査を行なうステップと、
審査の結果、会員資格有りの場合は、前記会員認証局から前記申込者に暗号鍵生成プログラムを内蔵したＩＣカードを配布するステップと、
該ＩＣカード中で、申込者の公開鍵と秘密鍵を生成するとともに、生成した公開鍵を含む申込者に関する所定の情報を所定のフォーマットでまとめたデータである会員証を作成するステップと、
前記申込者の端末から前記会員認証局の端末に、前記会員証を送信するステップと、
前記会員認証局の端末で、前記申込者の公開鍵を含む会員証が確かにその者のものであることを証明する証明書を作成して、申込者の端末に送信するステップと、
前記申込者の端末で、受信した証明書を前記ＩＣカードに格納するステップとを備えたことを特徴とする電子認証方法。
【請求項１３】会員認証局の端末と、個人認証局の端末と、会員の端末とが、ネットワークを介して相互に接続されているシステムに適用する電子認証方法であって、
前記会員の端末から前記会員認証局の端末に、個人認証書と会員証とを添付して会員登録の抹消の申込みを送信するステップと、
前記会員認証局の端末から前記個人認証局の端末に、受信した個人認証書の有効性の確認依頼を送信するステップと、
前記個人認証局の端末で、受信した個人認証書の有効性を確認し、確認結果を前記会員認証局の端末に送信するステップと、
前記会員認証局の端末で、受信した会員証の有効性を確認し、該会員証の有効性の確認結果および前記個人認証書の有効性の確認結果に基づいて、本人からの登録抹消依頼であることを確認した上で、会員登録の抹消を行なうステップとを備えたことを特徴とする電子認証方法。
【請求項１４】会員認証局の端末と、個人認証局の端末と、会員の端末とが、ネットワークを介して相互に接続されているシステムに適用する電子認証方法であって、
前記会員の端末から前記会員認証局の端末に、個人認証書と会員証とを添付して会員登録の有効性の確認依頼を

送信するステップと、
前記会員認証局の端末から前記個人認証局の端末に、受信した個人認証書の有効性の確認依頼を送信するステップと、
前記個人認証局の端末で、受信した個人認証書の有効性を確認し、確認結果を前記会員認証局の端末に送信するステップと、
前記会員認証局の端末で、受信した会員証の有効性を確認し、該会員証の有効性の確認結果および前記個人認証書の有効性の確認結果に基づいて、前記個人認証書と会員証で特定される会員の会員登録の有効性を確認し、その確認結果を前記会員の端末に送信するステップとを備えたことを特徴とする電子認証方法。
【請求項15】団体の構成員の端末が該団体内ネットワークを介して相互に接続され、該団体の構成員である登録責任者の端末が認証機関の端末とネットワークを介して相互に接続されているシステムにおいて、該団体の構成員の公開鍵の認証機関への登録および認証機関から証明書を発行してもらう処理を、該団体の登録責任者が代行して行なう電子認証方法であって、
公開鍵の登録を申請する構成員の端末において、その構成員が登録しようとしている公開鍵を認証機関の公開鍵で暗号化して、前記登録責任者の端末に送信するステップと、
前記登録責任者の端末において、受信した構成員の暗号化公開鍵に登録責任者のディジタル署名を付して、前記認証機関の端末に送信するステップと、
前記認証機関の端末において、前記登録責任者の端末から送信されたディジタル署名付きの暗号化公開鍵を受信し、前記登録責任者のディジタル署名を確認した後、前記認証機関の秘密鍵で該暗号化公開鍵を復号し、復号した公開鍵の証明書を作成し、該証明書を前記団体の公開鍵および／または前記構成員の公開鍵で暗号化して、前記登録責任者の端末または前記構成員の端末に送信するステップとを備えたことを特徴とする電子認証方法。
【請求項16】公証サービスを提供するサービス提供者が使用するサービス提供装置と、公証サービスを享受する複数のサービス享受者がそれぞれ使用する複数のサービス享受装置とが、ネットワークを介して相互に接続されて構成される電子認証公証システムであって、
前記サービス提供装置から、契約内容を含む契約情報を、契約者である各サービス享受者のサービス享受装置に、それぞれ送信し、
該契約情報を受信した各サービス享受装置で、該契約情報にサービス享受者の署名を付けた一者署名付き契約情報を作成して、前記サービス提供装置に送信し、前記サービス提供装置で、前記各サービス享受装置からそれぞれ送信された一者署名付き契約情報を受信し、受信した複数の一者署名付き契約情報をまとめて一つの文書にするとともに、該文書にサービス提供者の署名を付けたサービス提供者署名付き契約情報を作成し、該作成したサービス提供者署名付き契約情報を保管するとともに、前記各サービス享受装置に送信することを特徴とする電子認証公証システム。
【請求項17】公証サービスを提供するサービス提供者が使用するサービス提供装置と、公証サービスを享受する複数のサービス享受者が使用する複数のサービス享受装置と、前記サービス提供者および各サービス享受者の公開鍵が確かにその者の公開鍵であることを保証する証明書を発行する認証機関の端末装置とが、ネットワークを介して相互に接続されて構成される電子認証公証システムであって、
前記サービス提供装置で、前記サービス提供者の公開鍵と秘密鍵とを生成し、
前記各サービス享受装置で、それぞれ、前記各サービス享受者の公開鍵と秘密鍵とを生成し、
前記サービス提供装置および各サービス享受装置から、生成した公開鍵を前記認証機関の端末装置に送信し、
前記認証機関の端末装置で、受信した公開鍵ごとに、その公開鍵に対応する証明書を作成し、それぞれ対応する前記サービス提供装置および各サービス享受装置に送信し、
前記サービス提供装置および各サービス享受装置で、前記証明書をそれぞれ受信し、
前記各サービス享受装置から、それぞれ、契約内容その他の契約に係る各種の情報を前記サービス提供装置に送信し、
前記サービス提供装置において、前記各サービス享受装置からそれぞれ送られてくる契約に係る各種の情報をまとめて契約内容を含む契約情報を作成し、前記各サービス享受装置にそれぞれ送信し、
前記各サービス享受装置で、それぞれ、受信した契約情報にサービス享受者の証明書を含む付属情報を所定の順序で連結したデータを作成し、該連結したデータを所定の一方向性関数で圧縮した圧縮子を生成し、該圧縮子をサービス享受者の秘密鍵で暗号化した署名を生成し、前記連結したデータに該署名を合わせて一者署名付き契約情報を作成し、該一者署名付き契約情報を前記サービス提供装置に送信し、
前記サービス提供装置で、前記各サービス享受装置からそれぞれ送信された一者署名付き契約情報を受信し、受信した複数の一者署名付き契約情報から契約情報並びに各サービス享受者が付加した付属情報および署名を取り出し、取り出した情報とサービス提供者の証明書を含む付属情報とを所定の順序で連結したデータを作成し、該連結したデータを所定の一方向性関数で圧縮した圧縮子を生成し、該圧縮子をサービス提供者の秘密鍵で暗号化した署名を生成し、前記連結したデータに該署名を合わせてサービス提供者署名付き契約情報を作成し、
前記サービス提供装置で、作成したサービス提供者署名

付き契約情報を保管し、
前記サービス提供者署名付き契約情報を、前記サービス提供装置から前記各サービス享受装置に送信することを特徴とする電子認証公証システム。
【請求項18】前記ネットワークを介したサービス提供者およびサービス享受者と認証機関との間の通信は、認証機関の公開鍵と公開鍵暗号とを使用して鍵交換を行ない、その交換した鍵と共通鍵暗号とを使用した暗号通信により行なう請求項17に記載の電子認証公証システム。
【請求項19】前記ネットワークを介したサービス提供者とサービス享受者との間の通信は、互いの証明書を交換し、サービス提供者の公開鍵と公開鍵暗号とを使用して鍵交換を行ない、その交換した鍵と共通鍵暗号とを使用した暗号通信により行なう請求項16または17の何れか1つに記載の電子認証公証システム。
【請求項20】前記サービス提供者および各サービス享受者には、前記認証機関の公開鍵である認証機関証明書が格納されている、前記サービス提供装置およびサービス享受装置に着脱可能な、記憶媒体が、あらかじめ配布されており、
前記サービス提供者および各サービス享受者の公開鍵および秘密鍵、並びに、前記認証機関が発行した証明書は、該記憶媒体に格納される請求項16または17の何れか1つに記載の電子認証公証システム。
【請求項21】前記着脱可能な記憶媒体が、秘密鍵と公開鍵を生成する暗号鍵生成プログラムおよび入力したデータを秘密鍵で暗号化して署名を生成し出力するディジタル署名生成プログラム、並びにそれらのプログラムを実行して暗号鍵生成や署名生成を実行する処理装置を備えたICカードであり、
前記サービス提供者および各サービス享受者は、該ICカードを用いて、秘密鍵と公開鍵の生成、および署名の生成を行なうとともに、生成した秘密鍵と公開鍵および前記認証機関から送付された証明書は該ICカードに格納する請求項20に記載の電子認証公証システム。
【請求項22】前記着脱可能な記憶媒体には、当該記憶媒体の正当な使用者のパスワードで暗号化された暗号化秘密鍵、暗号化公開鍵、および暗号化自証明書、並びに該パスワードをチェックするためのパスワードチェック用データが格納され、上記暗号化秘密鍵、暗号化公開鍵、および暗号化自証明書にアクセスする際には、使用者が入力したパスワードを上記パスワードチェック用データを用いてチェックし、正当な使用者であると確認された場合のみアクセスを許可する請求項20に記載の電子認証公証システム。
【請求項23】前記着脱可能な記憶媒体が、内蔵時計、秘密鍵と公開鍵を生成する暗号鍵生成プログラムおよび入力したデータを秘密鍵で暗号化して署名を生成し出力するディジタル署名生成プログラム、並びにそれらのプログラムを実行して暗号鍵生成や署名生成を実行する処理装置を備えたICカードであり、
前記サービス提供者および各サービス享受者は、該ICカードを用いて、秘密鍵と公開鍵の生成および署名の生成を行なうとともに、生成した秘密鍵と公開鍵および前記認証機関から送付された証明書は該ICカードに格納し、署名生成時には署名対象のデータに上記内蔵時計の日時データを付加したデータを秘密鍵で暗号化して署名生成する請求項20に記載の電子認証公証システム。
【請求項24】前記ICカードは、署名生成の直前に、時刻管理機関が送信する正確な時刻を示す標準時刻データを受信し、該標準時刻データに基づいて内蔵時計を調整する請求項23に記載の電子認証公証システム。
【請求項25】前記ICカードは無線受信装置を備え、該無線受信装置により受信した前記時刻管理機関からの標準時刻データに基づいて内蔵時計を調整する請求項24に記載の電子認証公証システム。
【請求項26】前記着脱可能な記憶媒体内の秘密鍵、公開鍵、および証明書を用いて署名を行なったとき署名履歴を該記憶媒体内に記憶しておくとともに、該記憶媒体内の秘密鍵、公開鍵、および証明書が新たなデータに変更されたとき、署名履歴を参照して必要があれば、以前に使用した秘密鍵、公開鍵、および証明書を別領域に記憶しておく請求項20に記載の電子認証公証システム。
【請求項27】会員認証局の端末と、個人認証局の端末と、申込者の端末とが、ネットワークを介して相互に接続されて構成される電子認証システムであって、
あらかじめ、各申込者に対し、その申込者の公開鍵とその公開鍵がその申込者のものであることを証明する証明書とを含むディジタルデータである個人認証書が前記個人認証局から配布されており、
前記申込者の端末から前記会員認証局の端末に、個人認証書を添付した会員登録申込書を送信し、
前記会員認証局の端末から前記個人認証局の端末に、受信した個人認証書の有効性の確認依頼を送信し、
前記個人認証局の端末で、受信した個人認証書の有効性を確認し、確認結果を前記会員認証局の端末に送信し、
前記会員認証局の端末で、その確認結果に基づいて前記申込者の会員資格の審査を行ない、
審査の結果、会員資格有りの場合は、前記会員認証局から前記申込者に暗号鍵生成プログラムを内蔵したICカードを配布し、
該ICカード中で、申込者の公開鍵と秘密鍵を生成するとともに、生成した公開鍵を含む申込者に関する所定の情報を所定のフォーマットでまとめたデータである会員証を作成し、
前記申込者の端末から前記会員認証局の端末に、前記会員証を送信し、
前記会員認証局の端末で、前記申込者の公開鍵を含む会員証が確かにその者のものであることを証明する証明書

を作成して、申込者の端末に送信し、
前記申込者の端末で、受信した証明書を前記ＩＣカードに格納することを特徴とする電子認証システム。
【請求項２８】会員認証局の端末と、個人認証局の端末と、会員の端末とが、ネットワークを介して相互に接続されて構成される電子認証システムであって、
前記会員の端末から前記会員認証局の端末に、個人認証書と会員証とを添付して会員登録の抹消の申込みを送信し、
前記会員認証局の端末から前記個人認証局の端末に、受信した個人認証書の有効性の確認依頼を送信し、
前記個人認証局の端末で、受信した個人認証書の有効性を確認し、確認結果を前記会員認証局の端末に送信し、
前記会員認証局の端末で、受信した会員証の有効性を確認し、該会員証の有効性の確認結果および前記個人認証書の有効性の確認結果に基づいて、本人からの登録抹消依頼であることを確認した上で、会員登録の抹消を行なうことを特徴とする電子認証システム。
【請求項２９】会員認証局の端末と、個人認証局の端末と、会員の端末とが、ネットワークを介して相互に接続されて構成される電子認証システムであって、
前記会員の端末から前記会員認証局の端末に、個人認証書と会員証とを添付して会員登録の有効性の確認依頼を送信し、
前記会員認証局の端末から前記個人認証局の端末に、受信した個人認証書の有効性の確認依頼を送信し、
前記個人認証局の端末で、受信した個人認証書の有効性を確認し、確認結果を前記会員認証局の端末に送信し、
前記会員認証局の端末で、受信した会員証の有効性を確認し、該会員証の有効性の確認結果および前記個人認証書の有効性の確認結果に基づいて、前記個人認証書と会員証で特定される会員の会員登録の有効性を確認し、その確認結果を前記会員の端末に送信することを特徴とする電子認証システム。
【請求項３０】団体の構成員の端末が該団体内ネットワークを介して相互に接続され、該団体の構成員である登録責任者の端末が認証機関の端末とネットワークを介して相互に接続されているシステムにおいて、該団体の構成員の公開鍵の認証機関への登録および認証機関から証明書を発行してもらう処理を、該団体の登録責任者が代行して行なう電子認証システムであって、
公開鍵の登録を申請する構成員の端末において、その構成員が登録しようとしている公開鍵を認証機関の公開鍵で暗号化して、前記登録責任者の端末に送信し、
前記登録責任者の端末において、受信した構成員の暗号化公開鍵に登録責任者のディジタル署名を付して、前記認証機関の端末に送信し、
前記認証機関の端末において、前記登録責任者の端末から送信されたディジタル署名付きの暗号化公開鍵を受信し、前記登録責任者のディジタル署名を確認した後、前記認証機関の秘密鍵で該暗号化公開鍵を復号し、復号した公開鍵の証明書を作成し、該証明書を前記団体の公開鍵および／または前記構成員の公開鍵で暗号化して、前記登録責任者の端末または前記構成員の端末に送信することを特徴とする電子認証システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、電子認証公証方法およびそのシステムに関する。
【０００２】
【従来の技術】近年、インターネットのようなオープンなネットワーク環境において、暗号技術を用いた安全な電子商取引が行われるようになってきた。
【０００３】一般に、情報の暗号化に際しては、暗号アルゴリズムと暗号鍵とが必要である。暗号アルゴリズムとは、平文と呼ばれる誰でも正しい内容を理解できる情報を、暗号文と呼ばれる全く意味の分からない形の情報に変換する処理手順（暗号化）、およびその逆変換を行う処理手順（復号化）のことである。暗号鍵とは、上記暗号アルゴリズムの変換処理で使用する制御パラメータである。同じ暗号アルゴリズムを使って平文を暗号化しても、その際に使用する暗号鍵が異なると異なる暗号文に変換される。そのため、ある暗号文をもとの平文に正しく復号化するためには、暗号化時に使用したものと同じ暗号鍵、あるいは暗号化時に使用した暗号鍵と対になった暗号鍵が必要となる。前者のように、暗号化時と復号化時に全く同じ暗号鍵を使用する暗号アルゴリズムを対称鍵暗号、あるいは共通鍵暗号といい、後者のように、暗号化時と復号化時に異なる暗号鍵を使用する暗号アルゴリズムを非対称鍵暗号、あるいは公開鍵暗号という。
【０００４】共通鍵暗号は、処理速度が高速であるが、鍵の管理に手間がかかる。一方、公開鍵暗号は、処理速度は遅いが、鍵の管理が容易であり、またディジタル署名にも利用できる。
【０００５】すなわち、公開鍵暗号では、暗号化および復号化に使用する二つの暗号鍵の非対称性により、一方の鍵（公開鍵）を公に（すべての人に開示）することが可能である。そのため、共通鍵暗号に比べて暗号鍵の管理が比較的容易であり、かつ、認証のためのディジタル署名に利用可能であるといった利点もある。しかし、公開鍵暗号の運用に際しては、それら公にされた公開鍵とその所有者との対応関係が保証されなければならない。なぜなら、もし不正者ＡがユーザＢになりすましてＢの公開鍵を公にした場合（その公開鍵に対応した秘密鍵はＡが所有している）、ユーザＣは、電子署名を確認することにより不正者ＡをユーザＢだと認証してしまうからである。さらに、その結果として、ユーザＢに宛てた情報がすべて不正者Ａに漏れてしまうことになる。したがって、公開鍵暗号利用環境を構築する際には、公開鍵と

その所有者との対応関係を保証する手段が必要となる。

【０００６】認証局（Certification Authority）は、インターネットのように大規模でオープンなネットワークにおいて、このような課題を解決する手段の一つであり、CCITT（The International Telegraph and Telephone Consultative Committee）の勧告X.509で認証局と証明書を用いた認証の枠組みが規定されている。証明書とは、その証明書の所有者の公開鍵であり、他のいくつかの情報とともに、それを発行した認証局の秘密鍵を用いた暗号化、すなわちディジタル署名により、偽造不可能な形にしたデータのことである。システムを利用するすべてのエンティティは、認証局の証明書（公開鍵）だけを安全に保持し、他のエンティティの証明書に付けられた認証局のディジタル署名を確認することで、その証明書に含まれた公開鍵の正当性の確認および認証を行なうことが可能となる。

【０００７】

【発明が解決しようとする課題】ところで、インターネットのようなネットワーク環境における電子商取引は、消費者－販売店（モール）間での電子商取引から、企業－企業間の電子商取引へと拡大していく兆しがある。企業間電子商取引では、個々の取引を安全に行なうだけでなく、取引内容やそのような取引が行なわれたという事実を保証し、その証拠をある一定の期間保管しておく“公証サービス”の重要性が高まっていくものと考えられる。また、そのような公証サービスは、消費者電子商取引への適用や、電子商取引以外への適用（遺言等、現在公証人役場で公証人が提供しているサービス）も考えられる。

【０００８】しかしながら、ＩＳＯでは、“否認防止（Non Repudiation）”技術の標準化は進められているが、フレームワーク的なものであり、実現方式を細かく規定したものとはなっていない。また、オンラインで受け取った電子情報を保管するサービスはあるが（電子貸し金庫）、取引という観点がないため、上記“公証サービス”は実現できない。さらに、法務省民事部が電子取引における電子認証・公証制度の必要性を提言しているが、これも実現方式を細かく規定したものではない。

【０００９】本発明は、オープンなネットワーク環境において電子商取引を行なう際に必要とされる認証・公証サービス（電子情報署名・保管サービス）を実現することを目的とする。

【００１０】

【課題を解決するための手段】上記目的を達成するため、請求項１に係る発明は、公証サービスを提供するサービス提供者が使用するサービス提供装置と、公証サービスを享受する複数のサービス享受者がそれぞれ使用する複数のサービス享受装置とが、ネットワークを介して相互に接続されているシステムに適用する電子認証公証方法であって、前記サービス提供装置から、契約内容を含む契約情報を、契約者である各サービス享受者のサービス享受装置に、それぞれ送信するステップと、該契約情報を受信した各サービス享受装置で、該契約情報にサービス享受者の署名を付けた一者署名付き契約情報を作成し、前記サービス提供装置に送信するステップと、前記サービス提供装置で、前記各サービス享受装置からそれぞれ送信された一者署名付き契約情報を受信し、受信した複数の一者署名付き契約情報をまとめて一つの文書にするとともに、該文書にサービス提供者の署名を付けたサービス提供者署名付き契約情報を作成するステップと、前記サービス提供装置で、作成したサービス提供者署名付き契約情報を保管するステップと、前記サービス提供者署名付き契約情報を、前記サービス提供装置から前記各サービス享受装置に送信するステップとを備えたことを特徴とする。

【００１１】請求項２に係る発明は、公証サービスを提供するサービス提供者が使用するサービス提供装置と、公証サービスを享受する複数のサービス享受者が使用する複数のサービス享受装置と、前記サービス提供者および各サービス享受者の公開鍵が確かにその者の公開鍵であることを保証する証明書を発行する認証機関の端末装置とが、ネットワークを介して相互に接続されているシステムに適用する電子認証公証方法であって、前記サービス提供装置で、前記サービス提供者の公開鍵と秘密鍵とを生成するステップと、前記各サービス享受装置で、それぞれ、前記各サービス享受者の公開鍵と秘密鍵とを生成するステップと、前記サービス提供装置および各サービス享受装置から、生成した公開鍵を前記認証機関の端末装置に送信するステップと、前記認証機関の端末装置で、受信した公開鍵ごとに、その公開鍵に対応する証明書を作成し、それぞれ対応する前記サービス提供装置および各サービス享受装置に送信するステップと、前記サービス提供装置および各サービス享受装置で、前記証明書をそれぞれ受信するステップと、前記各サービス享受装置から、それぞれ、契約内容その他の契約に係る各種の情報を前記サービス提供装置に送信するステップと、前記サービス提供装置において、前記各サービス享受装置からそれぞれ送られてくる契約に係る各種の情報をまとめて契約内容を含む契約情報を作成し、前記各サービス享受装置にそれぞれ送信するステップと、前記各サービス享受装置で、それぞれ、受信した契約情報にサービス享受者の証明書を含む付属情報を所定の順序で連結したデータを作成し、該連結したデータを所定の一方向性関数で圧縮した圧縮子を生成し、該圧縮子をサービス享受者の秘密鍵で暗号化した署名を生成し、前記連結したデータに該署名を合わせて一者署名付き契約情報を作成し、該一者署名付き契約情報を前記サービス提供装置に送信するステップと、前記サービス提供装置で、前記各サービス享受装置からそれぞれ送信された一者署名付き契約情報を受信し、受信した複数の一者署名付き契

約情報から契約情報並びに各サービス享受者が付加した付属情報および署名を取り出し、取り出した情報とサービス提供者の証明書を含む付属情報とを所定の順序で連結したデータを作成し、該連結したデータを所定の一方向性関数で圧縮した圧縮子を生成し、該圧縮子をサービス提供者の秘密鍵で暗号化した署名を生成し、前記連結したデータに該署名を合わせてサービス提供者署名付き契約情報を作成するステップと、前記サービス提供装置で、作成したサービス提供者署名付き契約情報を保管するステップと、前記サービス提供者署名付き契約情報を、前記サービス提供装置から前記各サービス享受装置に送信するステップとを備えたことを特徴とする。

【００１２】請求項３に係る発明は、請求項２において、前記ネットワークを介したサービス提供者およびサービス享受者と認証機関との間の通信を、認証機関の公開鍵と公開鍵暗号とを使用して鍵交換を行ない、その交換した鍵と共通鍵暗号とを使用した暗号通信により行なうこととしたものである。

【００１３】請求項４に係る発明は、請求項１または２において、前記ネットワークを介したサービス提供者とサービス享受者との間の通信を、互いの証明書を交換し、サービス提供者の公開鍵と公開鍵暗号とを使用して鍵交換を行ない、その交換した鍵と共通鍵暗号とを使用した暗号通信により行なうこととしたものである。

【００１４】請求項５に係る発明は、請求項１または２において、前記サービス提供者および各サービス享受者には、前記認証機関の公開鍵である認証機関証明書が格納されている、前記サービス提供装置およびサービス享受装置に着脱可能な、記憶媒体が、あらかじめ配布されており、前記サービス提供者および各サービス享受者の公開鍵および秘密鍵、並びに、前記認証機関が発行した証明書は、該記憶媒体に格納されることとしたものである。

【００１５】請求項６に係る発明は、請求項５において、前記着脱可能な記憶媒体が、秘密鍵と公開鍵を生成する暗号鍵生成プログラムおよび入力したデータを秘密鍵で暗号化して署名を生成し出力するディジタル署名生成プログラム、並びにそれらのプログラムを実行して暗号鍵生成や署名生成を実行する処理装置を備えたＩＣカードであり、前記サービス提供者および各サービス享受者は、該ＩＣカードを用いて、秘密鍵と公開鍵の生成、および署名の生成を行なうとともに、生成した秘密鍵と公開鍵および前記認証機関から送付された証明書は該ＩＣカードに格納することとしたものである。

【００１６】請求項７に係る発明は、請求項５において、前記着脱可能な記憶媒体には、当該記憶媒体の正当な使用者のパスワードで暗号化された暗号化秘密鍵、暗号化公開鍵、および暗号化自証明書、並びに該パスワードをチェックするためのパスワードチェック用データが格納され、上記暗号化秘密鍵、暗号化公開鍵、および暗号化自証明書にアクセスする際には、使用者が入力したパスワードを上記パスワードチェック用データを用いてチェックし、正当な使用者であると確認された場合のみアクセスを許可することとしたものである。

【００１７】請求項８に係る発明は、請求項５において、前記着脱可能な記憶媒体が、内蔵時計、秘密鍵と公開鍵を生成する暗号鍵生成プログラムおよび入力したデータを秘密鍵で暗号化して署名を生成し出力するディジタル署名生成プログラム、並びにそれらのプログラムを実行して暗号鍵生成や署名生成を実行する処理装置を備えたＩＣカードであり、前記サービス提供者および各サービス享受者は、該ＩＣカードを用いて、秘密鍵と公開鍵の生成および署名の生成を行なうとともに、生成した秘密鍵と公開鍵および前記認証機関から送付された証明書は該ＩＣカードに格納し、署名生成時には署名対象のデータに上記内蔵時計の日時データを付加したデータを秘密鍵で暗号化して署名生成することとしたものである。

【００１８】請求項９に係る発明は、請求項８において、前記ＩＣカードが、署名生成の直前に、時刻管理機関が送信する正確な時刻を示す標準時刻データを受信し、該標準時刻データに基づいて内蔵時計を調整することとしたものである。

【００１９】請求項１０に係る発明は、請求項９において、前記ＩＣカードは無線受信装置を備え、該無線受信装置により受信した前記時刻管理機関からの標準時刻データに基づいて内蔵時計を調整することとしたものである。

【００２０】請求項１１に係る発明は、請求項５において、前記着脱可能な記憶媒体内の秘密鍵、公開鍵、および証明書を用いて署名を行なったとき署名履歴を該記憶媒体内に記憶しておくとともに、該記憶媒体内の秘密鍵、公開鍵、および証明書が新たなデータに変更されたとき、署名履歴を参照して必要があれば、以前に使用した秘密鍵、公開鍵、および証明書を別領域に記憶しておくこととしたものである。

【００２１】請求項１２に係る発明は、会員認証局の端末と、個人認証局の端末と、申込者の端末とが、ネットワークを介して相互に接続されているシステムに適用する電子認証方法であって、あらかじめ、各申込者が、その申込者の公開鍵とその公開鍵がその申込者のものであることを証明する証明書とを含むディジタルデータである個人認証書の配布を前記個人認証局から受けるステップと、前記申込者の端末から前記会員認証局の端末に、個人認証書を添付した会員登録申込書を送信するステップと、前記会員認証局の端末から前記個人認証局の端末に、受信した個人認証書の有効性の確認依頼を送信するステップと、前記個人認証局の端末で、受信した個人認証書の有効性を確認し、確認結果を前記会員認証局の端末に送信するステップと、前記会員認証局の端末で、そ

の確認結果に基づいて前記申込者の会員資格の審査を行なうステップと、審査の結果、会員資格有りの場合は、前記会員認証局から前記申込者に暗号鍵生成プログラムを内蔵したＩＣカードを配布するステップと、該ＩＣカード中で、申込者の公開鍵と秘密鍵を生成するとともに、生成した公開鍵を含む申込者に関する所定の情報を所定のフォーマットでまとめたデータである会員証を作成するステップと、前記申込者の端末から前記会員認証局の端末に、前記会員証を送信するステップと、前記会員認証局の端末で、前記申込者の公開鍵を含む会員証が確かにその者のものであることを証明する証明書を作成して、申込者の端末に送信するステップと、前記申込者の端末で、受信した証明書を前記ＩＣカードに格納するステップとを備えたことを特徴とする。

【００２２】請求項１３に係る発明は、会員認証局の端末と、個人認証局の端末と、会員の端末とが、ネットワークを介して相互に接続されているシステムに適用する電子認証方法であって、前記会員の端末から前記会員認証局の端末に、個人認証書と会員証とを添付して会員登録の抹消の申込みを送信するステップと、前記会員認証局の端末から前記個人認証局の端末に、受信した個人認証書の有効性の確認依頼を送信するステップと、前記個人認証局の端末で、受信した個人認証書の有効性を確認し、確認結果を前記会員認証局の端末に送信するステップと、前記会員認証局の端末で、受信した会員証の有効性を確認し、該会員証の有効性の確認結果および前記個人認証書の有効性の確認結果に基づいて、本人からの登録抹消依頼であることを確認した上で、会員登録の抹消を行なうステップとを備えたことを特徴とする。

【００２３】請求項１４に係る発明は、会員認証局の端末と、個人認証局の端末と、会員の端末とが、ネットワークを介して相互に接続されているシステムに適用する電子認証方法であって、前記会員の端末から前記会員認証局の端末に、個人認証書と会員証とを添付して会員登録の有効性の確認依頼を送信するステップと、前記会員認証局の端末から前記個人認証局の端末に、受信した個人認証書の有効性の確認依頼を送信するステップと、前記個人認証局の端末で、受信した個人認証書の有効性を確認し、確認結果を前記会員認証局の端末に送信するステップと、前記会員認証局の端末で、受信した会員証の有効性を確認し、該会員証の有効性の確認結果および前記個人認証書の有効性の確認結果に基づいて、前記個人認証書と会員証で特定される会員の会員登録の有効性を確認し、その確認結果を前記会員の端末に送信するステップとを備えたことを特徴とする。

【００２４】請求項１５に係る発明は、団体の構成員の端末が該団体内ネットワークを介して相互に接続され、該団体の構成員である登録責任者の端末が認証機関の端末とネットワークを介して相互に接続されているシステムにおいて、該団体の構成員の公開鍵の認証機関への登録および認証機関から証明書を発行してもらう処理を、該団体の登録責任者が代行して行なう電子認証方法であって、公開鍵の登録を申請する構成員の端末において、その構成員が登録しようとしている公開鍵を認証機関の公開鍵で暗号化して、前記登録責任者の端末に送信するステップと、前記登録責任者の端末において、受信した構成員の暗号化公開鍵に登録責任者のディジタル署名を付して、前記認証機関の端末に送信するステップと、前記認証機関の端末において、前記登録責任者の端末から送信されたディジタル署名付きの暗号化公開鍵を受信し、前記登録責任者のディジタル署名を確認した後、前記認証機関の秘密鍵で該暗号化公開鍵を復号し、復号した公開鍵の証明書を作成し、該証明書を前記団体の公開鍵および／または前記構成員の公開鍵で暗号化して、前記登録責任者の端末または前記構成員の端末に送信するステップとを備えたことを特徴とする。

【００２５】請求項１６に係る発明は、公証サービスを提供するサービス提供者が使用するサービス提供装置と、公証サービスを享受する複数のサービス享受者がそれぞれ使用する複数のサービス享受装置とが、ネットワークを介して相互に接続されて構成される電子認証公証システムであって、前記サービス提供装置から、契約内容を含む契約情報を、契約者である各サービス享受者のサービス享受装置に、それぞれ送信し、該契約情報を受信した各サービス享受装置で、該契約情報にサービス享受者の署名を付けた一者署名付き契約情報を作成して、前記サービス提供装置に送信し、前記サービス提供装置で、前記各サービス享受装置からそれぞれ送信された一者署名付き契約情報を受信し、受信した複数の一者署名付き契約情報をまとめて一つの文書にするとともに、該文書にサービス提供者の署名を付けたサービス提供者署名付き契約情報を作成し、該作成したサービス提供者署名付き契約情報を保管するとともに、前記各サービス享受装置に送信することを特徴とする。

【００２６】請求項１７に係る発明は、公証サービスを提供するサービス提供者が使用するサービス提供装置と、公証サービスを享受する複数のサービス享受者が使用する複数のサービス享受装置と、前記サービス提供者および各サービス享受者の公開鍵が確かにその者の公開鍵であることを保証する証明書を発行する認証機関の端末装置とが、ネットワークを介して相互に接続されて構成される電子認証公証システムであって、前記サービス提供装置で、前記サービス提供者の公開鍵と秘密鍵とを生成し、前記各サービス享受装置で、それぞれ、前記各サービス享受者の公開鍵と秘密鍵とを生成し、前記サービス提供装置および各サービス享受装置から、生成した公開鍵を前記認証機関の端末装置に送信し、前記認証機関の端末装置で、受信した公開鍵ごとに、その公開鍵に対応する証明書を作成し、それぞれ対応する前記サービス提供装置および各サービス享受装置に送信し、前記サ

ービス提供装置および各サービス享受装置で、前記証明書をそれぞれ受信し、前記各サービス享受装置から、それぞれ、契約内容その他の契約に係る各種の情報を前記サービス提供装置に送信し、前記サービス提供装置において、前記各サービス享受装置からそれぞれ送られてくる契約に係る各種の情報をまとめて契約内容を含む契約情報を作成し、前記各サービス享受装置にそれぞれ送信し、前記各サービス享受装置で、それぞれ、受信した契約情報にサービス享受者の証明書を含む付属情報を所定の順序で連結したデータを作成し、該連結したデータを所定の一方向性関数で圧縮した圧縮子を生成し、該圧縮子をサービス享受者の秘密鍵で暗号化した署名を生成し、前記連結したデータに該署名を合わせて一者署名付き契約情報を作成し、該一者署名付き契約情報を前記サービス提供装置に送信し、前記サービス提供装置で、前記各サービス享受装置からそれぞれ送信された一者署名付き契約情報を受信し、受信した複数の一者署名付き契約情報から契約情報並びに各サービス享受者が付加した付属情報および署名を取り出し、取り出した情報とサービス提供者の証明書を含む付属情報とを所定の順序で連結したデータを作成し、該連結したデータを所定の一方向性関数で圧縮した圧縮子を生成し、該圧縮子をサービス提供者の秘密鍵で暗号化した署名を生成し、前記連結したデータに該署名を合わせてサービス提供者署名付き契約情報を作成し、前記サービス提供装置で、作成したサービス提供者署名付き契約情報を保管し、前記サービス提供者署名付き契約情報を、前記サービス提供装置から前記各サービス享受装置に送信することを特徴とする。

【００２７】請求項１８に係る発明は、請求項１７において、前記ネットワークを介したサービス提供者およびサービス享受者と認証機関との間の通信を、認証機関の公開鍵と公開鍵暗号とを使用して鍵交換を行ない、その交換した鍵と共通鍵暗号とを使用した暗号通信により行なうこととしたものである。

【００２８】請求項１９に係る発明は、請求項１６または１７において、前記ネットワークを介したサービス提供者とサービス享受者との間の通信を、互いの証明書を交換し、サービス提供者の公開鍵と公開鍵暗号とを使用して鍵交換を行ない、その交換した鍵と共通鍵暗号とを使用した暗号通信により行なうこととしたものである。

【００２９】請求項２０に係る発明は、請求項１６または１７において、前記サービス提供者および各サービス享受者には、前記認証機関の公開鍵である認証機関証明書が格納されている、前記サービス提供装置およびサービス享受装置に着脱可能な、記憶媒体が、あらかじめ配布されており、前記サービス提供者および各サービス享受者の公開鍵および秘密鍵、並びに、前記認証機関が発行した証明書は、該記憶媒体に格納されることとしたものである。

【００３０】請求項２１に係る発明は、請求項２０において、前記着脱可能な記憶媒体が、秘密鍵と公開鍵を生成する暗号鍵生成プログラムおよび入力したデータを秘密鍵で暗号化して署名を生成し出力するディジタル署名生成プログラム、並びにそれらのプログラムを実行して暗号鍵生成や署名生成を実行する処理装置を備えたＩＣカードであり、前記サービス提供者および各サービス享受者は、該ＩＣカードを用いて、秘密鍵と公開鍵の生成、および署名の生成を行なうとともに、生成した秘密鍵と公開鍵および前記認証機関から送付された証明書は該ＩＣカードに格納することとしたものである。

【００３１】請求項２２に係る発明は、請求項２０において、前記着脱可能な記憶媒体には、当該記憶媒体の正当な使用者のパスワードで暗号化された暗号化秘密鍵、暗号化公開鍵、および暗号化自証明書、並びに該パスワードをチェックするためのパスワードチェック用データが格納され、上記暗号化秘密鍵、暗号化公開鍵、および暗号化自証明書にアクセスする際には、使用者が入力したパスワードを上記パスワードチェック用データを用いてチェックし、正当な使用者であると確認された場合のみアクセスを許可することとしたものである。

【００３２】請求項２３に係る発明は、請求項２０において、前記着脱可能な記憶媒体が、内蔵時計、秘密鍵と公開鍵を生成する暗号鍵生成プログラムおよび入力したデータを秘密鍵で暗号化して署名を生成し出力するディジタル署名生成プログラム、並びにそれらのプログラムを実行して暗号鍵生成や署名生成を実行する処理装置を備えたＩＣカードであり、前記サービス提供者および各サービス享受者は、該ＩＣカードを用いて、秘密鍵と公開鍵の生成および署名の生成を行なうとともに、生成した秘密鍵と公開鍵および前記認証機関から送付された証明書は該ＩＣカードに格納し、署名生成時には署名対象のデータに上記内蔵時計の日時データを付加したデータを秘密鍵で暗号化して署名生成することとしたものである。

【００３３】請求項２４に係る発明は、請求項２３において、前記ＩＣカードが、署名生成の直前に、時刻管理機関が送信する正確な時刻を示す標準時刻データを受信し、該標準時刻データに基づいて内蔵時計を調整することとしたものである。

【００３４】請求項２５に係る発明は、請求項２４において、前記ＩＣカードは無線受信装置を備え、該無線受信装置により受信した前記時刻管理機関からの標準時刻データに基づいて内蔵時計を調整することとしたものである。

【００３５】請求項２６に係る発明は、請求項２０において、前記着脱可能な記憶媒体内の秘密鍵、公開鍵、および証明書を用いて署名を行なったとき署名履歴を該記憶媒体内に記憶しておくとともに、該記憶媒体内の秘密鍵、公開鍵、および証明書が新たなデータに変更された

とき、署名履歴を参照して必要があれば、以前に使用した秘密鍵、公開鍵、および証明書を別領域に記憶しておくこととしたものである。

【００３６】請求項２７に係る発明は、会員認証局の端末と、個人認証局の端末と、申込者の端末とが、ネットワークを介して相互に接続されて構成される電子認証システムであって、あらかじめ、各申込者に対し、その申込者の公開鍵とその公開鍵がその申込者のものであることを証明する証明書とを含むディジタルデータである個人認証書が前記個人認証局から配布されており、前記申込者の端末から前記会員認証局の端末に、個人認証書を添付した会員登録申込書を送信し、前記会員認証局の端末から前記個人認証局の端末に、受信した個人認証書の有効性の確認依頼を送信し、前記個人認証局の端末で、受信した個人認証書の有効性を確認し、確認結果を前記会員認証局の端末に送信し、前記会員認証局の端末で、その確認結果に基づいて前記申込者の会員資格の審査を行ない、審査の結果、会員資格有りの場合は、前記会員認証局から前記申込者に暗号鍵生成プログラムを内蔵したＩＣカードを配布し、該ＩＣカード中で、申込者の公開鍵と秘密鍵を生成するとともに、生成した公開鍵を含む申込者に関する所定の情報を所定のフォーマットでまとめたデータである会員証を作成し、前記申込者の端末から前記会員認証局の端末に、前記会員証を送信し、前記会員認証局の端末で、前記申込者の公開鍵を含む会員証が確かにその者のものであることを証明する証明書を作成して、申込者の端末に送信し、前記申込者の端末で、受信した証明書を前記ＩＣカードに格納することを特徴とする。

【００３７】請求項２８に係る発明は、会員認証局の端末と、個人認証局の端末と、会員の端末とが、ネットワークを介して相互に接続されて構成される電子認証システムであって、前記会員の端末から前記会員認証局の端末に、個人認証書と会員証とを添付して会員登録の抹消の申込みを送信し、前記会員認証局の端末から前記個人認証局の端末に、受信した個人認証書の有効性の確認依頼を送信し、前記個人認証局の端末で、受信した個人認証書の有効性を確認し、確認結果を前記会員認証局の端末に送信し、前記会員認証局の端末で、受信した会員証の有効性を確認し、該会員証の有効性の確認結果および前記個人認証書の有効性の確認結果に基づいて、本人からの登録抹消依頼であることを確認した上で、会員登録の抹消を行なうことを特徴とする。

【００３８】請求項２９に係る発明は、会員認証局の端末と、個人認証局の端末と、会員の端末とが、ネットワークを介して相互に接続されて構成される電子認証システムであって、前記会員の端末から前記会員認証局の端末に、個人認証書と会員証とを添付して会員登録の有効性の確認依頼を送信し、前記会員認証局の端末から前記個人認証局の端末に、受信した個人認証書の有効性の確認依頼を送信し、前記個人認証局の端末で、受信した個人認証書の有効性を確認し、確認結果を前記会員認証局の端末に送信し、前記会員認証局の端末で、受信した会員証の有効性を確認し、該会員証の有効性の確認結果および前記個人認証書の有効性の確認結果に基づいて、前記個人認証書と会員証で特定される会員の会員登録の有効性を確認し、その確認結果を前記会員の端末に送信することを特徴とする。

【００３９】請求項３０に係る発明は、団体の構成員の端末が該団体内ネットワークを介して相互に接続され、該団体の構成員である登録責任者の端末が認証機関の端末とネットワークを介して相互に接続されているシステムにおいて、該団体の構成員の公開鍵の認証機関への登録および認証機関から証明書を発行してもらう処理を、該団体の登録責任者が代行して行なう電子認証システムであって、公開鍵の登録を申請する構成員の端末において、その構成員が登録しようとしている公開鍵を認証機関の公開鍵で暗号化して、前記登録責任者の端末に送信し、前記登録責任者の端末において、受信した構成員の暗号化公開鍵に登録責任者のディジタル署名を付して、前記認証機関の端末に送信し、前記認証機関の端末において、前記登録責任者の端末から送信されたディジタル署名付きの暗号化公開鍵を受信し、前記登録責任者のディジタル署名を確認した後、前記認証機関の秘密鍵で該暗号化公開鍵を復号し、復号した公開鍵の証明書を作成し、該証明書を前記団体の公開鍵および／または前記構成員の公開鍵で暗号化して、前記登録責任者の端末または前記構成員の端末に送信することを特徴とする。

【００４０】

【発明の実施の形態】以下、図面を用いて、本発明の実施の形態を説明する。

【００４１】図１は、本発明の第１の実施の形態に係る電子公証システムのシステム図である。同図において、１００は公証サービスを提供するサービス提供者、１３０はサービス提供者が使用するサービス提供装置、１１０と１１１は公証サービスを享受するサービス享受者、１４０と１４１はサービス享受者１１０と１１１がそれぞれ使用するサービス享受装置を示す。１００，１１０，１１１は擬人化して図示してあるが、自然人とは限らず、法人などの団体であってもよい。１７０は各者が本人であることを保証する証明書を発行する認証機関、１８０は本システムで用いるＩＣカード１２０を発行するＩＣカード発行機関である。

【００４２】サービス提供装置１３０およびサービス享受装置１４０，１４１は、通信網１８０に接続されており相互に各種情報の授受が可能である。また、図示していないが、認証機関１７０内に設けられた証明書発行業務を行なう端末装置が、上記通信網１８０に接続されており、サービス提供装置１３０およびサービス享受装置１４０，１４１と各種情報の授受が可能である。

【００４３】図１を参照して、本システムにおける公証サービスの流れを説明する。サービス享受者１１０と１１１との間には、あらかじめ何らかの契約を行なう合意が取れているものとする。サービスの前準備として、サービス享受者１１０，１１１とサービス提供者１００は、それぞれ、認証機関１７０に対してＩＣカード１２０の発行を申し込む。認証機関１７０は、ＩＣカード発行の申込みを受け付け、種々の方法でその申込者が本人であることを確認し、ＩＣカード１２０を発行する。ここでは、サービス提供者１００に対してＩＣカード１２１を、サービス享受者１１０に対してＩＣカード１２２を、サービス享受者１１１に対してＩＣカード１２３を、それぞれ発行したとする。なお、図１において、点線の矢印はオフラインで各者間のやり取りを行なうことを示し、実線の矢印は通信網１８０を介したオンラインでのやり取りを行なうことを示す。

【００４４】認証機関１７０はＩＣカード１２０をどのような方法で用意してもよいが、本システムで用いるＩＣカード（図２で後述）は規格化されたものであるので、ＩＣカード発行機関１８０が作成したＩＣカード１２０を用いることとしている。

【００４５】サービス提供者１００とサービス享受者１１０，１１１は、それぞれ、ＩＣカード１２１～１２３内に自分の公開鍵と秘密鍵を生成する作業を行う。ＩＣカードは、公開鍵と秘密鍵を生成する機能を備えている。次に各者１００，１１０，１１１は、それぞれ、生成した自分の公開鍵１５０，１５１，１５２を認証機関１７０に送り、証明書１５３，１５４，１５５を取得する。公開鍵１５０～１５２を送信して証明書１５３～１５５を取得する処理はオンラインで行なう。受信した証明書１５３～１５５は、それぞれ、各者１００，１１０，１１１のＩＣカード１２１～１２３に格納される。

【００４６】以上で、公証サービスを行なうための前準備を終える。

【００４７】公証サービスは以下のような手順で行なわれる。まず、所定の契約内容で契約することに合意しているサービス享受者１１０と１１１は、それぞれ、契約内容をサービス提供者１００にオンラインで（オフラインでもよい）送付する。サービス提供者１００は、その契約内容を総合して一定の書式にまとめた契約情報１６０を作成し、サービス享受者１１０，１１１にそれぞれオンラインで（オフラインでもよい）送付する。サービス享受者１１０，１１１は、それぞれ、その契約情報１６０の内容を確認し、依存がなければ、自分のＩＣカード１２２，１２３をサービス享受装置１４０，１４１に挿入して、契約情報１６０にディジタル署名を付ける。ＩＣカードは、署名生成機能を備えている。ここまでで、サービス享受者１１０側では一者署名付き契約情報１６１が作成され、サービス享受者１１１側では一者署名付き契約情報１６２が作成されたことになる。

【００４８】これらの一者署名付き契約情報１６１，１６２は、サービス享受装置１４０，１４１から、それぞれサービス提供装置１３０に返送される。サービス提供者１００は、サービス享受者１１０の署名が付いた一者署名付き契約情報１６１とサービス享受者１１１の署名が付いた一者署名付き契約情報１６２とを合わせて１つの文書にするとともに、該文書にＩＣカード１２１を用いてディジタル署名を付して、三者署名付き契約情報１６３を作成する。サービス提供者１００は、この三者署名付き契約情報１６３をサービス享受者１１０，１１１にそれぞれ送付するとともに、一定期間これを保管する。

【００４９】以上により、サービス提供者１００による公証サービス（サービス享受者１１０，１１１間の契約に係る公証）が行なわれた。サービス提供者１００は、三者署名付き契約情報１６３を一定期間保管しているので、この三者署名付き契約情報１６３がある限り、その契約内容および契約が行なわれた事実を保証できる。

【００５０】なお、図１ではサービス享受者が二者の場合を示したが、サービス享受者が三者以上いる場合も同様である。例えば、サービス享受者が三者いる場合は、サービス提供者はその三者から送られてくる一者署名付き契約情報を一文書にして自分の署名を付け、四者署名付き契約情報（サービス提供者署名付き契約情報）を作成して保管することになる。

【００５１】また、本実施の形態のシステムにおいて、サービス提供装置１３０やサービス享受装置１４０，１４１と認証機関１７０の端末装置とのオンラインでのデータのやり取り（証明書発行時）は、暗号通信で行なうものとする。すなわち、まず認証機関１７０の公開鍵（後述する認証機関証明書５１３）と公開鍵暗号とを使って鍵交換を行ない、その交換した鍵と共通鍵暗号とにより暗号通信を行なう。また、サービス提供装置１３０とサービス享受装置１４０，１４１とのオンラインでのデータのやり取り（公証サービス時）も、同様に暗号通信で行なうものとする。すなわち、まず、互いの証明書を交換し、次にサービス提供者１００の公開鍵と公開鍵暗号とを使って鍵交換を行ない、その交換した鍵と共通鍵暗号とにより暗号通信を行なう。上記暗号通信において、交換した鍵は一連のサービス終了まで使用する。

【００５２】図２は、図１のＩＣカード発行機関１８０が発行するＩＣカード１２０の内部構成図である。認証機関１７０がサービス提供者１００、およびサービス享受者１１０，１１１に配布するＩＣカード１２１～１２３はこの構成のものである。同図に示すように、ＩＣカード１２０は、リーダライタインタフェース２０１と、ＣＰＵ（中央処理装置）２０２と、メモリ２０３とを有している。これら各部はバス２００によって相互に接続されている。

【００５３】ＣＰＵ２０２は、演算機能を備え、ＩＣカ

ード１２０内の処理の全体を制御する。リーダライタインタフェース２０１は、後述する各者の装置のリーダライタ３２０，４２０との間でデータのやり取りを行なうためのインタフェースである。メモリ２０３には、端末・ＩＣカード間データ送受信プログラムが記憶されている領域２０３ａ、ＩＣカード制御プログラムが記憶されている領域２０３ｂ、暗号鍵生成プログラムが記憶されている領域２０３ｃ、署名生成プログラムが記憶されている領域２０３ｄ、およびデータ記憶領域２０３ｅが設けられている。メモリ２０３はこのＩＣカード１２０をリーダライタから引き抜いた状態でも記憶内容を保持する不揮発なメモリであり、ＣＰＵ２０２から見ると、プログラムを記憶した領域２０３ａ～２０３ｄは読み出しのみ可能な領域、データ記憶領域２０３ｅは読み出し・書き込みが可能な領域である。

【００５４】メモリ２０３に記憶されている端末・ＩＣカード間データ送受信プログラムは、リーダライタを介して当該ＩＣカードと端末との間でデータのやり取りを行なう際に使用するプログラムである。ＩＣカード制御プログラムは、このＩＣカード全体の動作を制御（データの流れの制御やアクセスコントロールなど）するプログラムである。暗号鍵生成プログラムは、秘密鍵と公開鍵を生成するプログラムである。署名生成プログラムは、外から与えられたデータに対してディジタル署名を付けて返す処理を行なうプログラムである。データ記憶領域２０３ｅに記憶するデータについては、図５で詳しく説明する。

【００５５】図３は、サービス提供装置１３０の内部構成図である。同図に示すように、サービス提供装置１３０は、端末３００、リーダライタ３２０、および外部記憶装置３４０を備えている。

【００５６】端末３００は、リーダライタインタフェース３１１、外部記憶装置インタフェース３１２、通信網インタフェース３１３、ＣＰＵ３１４、入出力装置３１５、およびメモリ３１６を備えている。これら各部は、バス３１０によって相互に接続されている。リーダライタインタフェース３１１は、リーダライタ３２０との間でデータのやり取りを行なうためのインタフェースである。外部記憶装置インタフェース３１２は、外部記憶装置３４０との間でデータのやり取りを行なうためのインタフェースである。通信網インタフェース３１３は、通信網１８０を介して別の端末との間でデータのやり取りを行なう際のインタフェースである。ＣＰＵ３１４は、演算機能を備え、このサービス提供装置１３０全体の動作を制御する。入出力装置３１５は、各種の情報を表示するディスプレイや、ユーザがコマンドやデータを入力するためのキーボードやマウスなどからなる。

【００５７】メモリ３１６には、端末・ＩＣカード間データ送受信プログラムが記憶されている領域３１６ａ、サービス提供プログラムが記憶されている領域３１６ｂ、通信プログラムが記憶されている領域３１６ｃ、暗号プログラムが記憶されている領域３１６ｄ、およびデータ記憶領域３１６ｅが設けられている。メモリ３１６は電源を落とすと内容が失われる揮発性のメモリでよい。メモリ３１６内のプログラムやデータは、必要に応じてハードディスクなどの外部記憶装置３４０から読み込まれ、保存が必要なデータは外部記憶装置３４０に書き込まれる。

【００５８】メモリ３１６に格納されている端末・ＩＣカード間データ送受信プログラムは、リーダライタ３２０を介して当該端末３００とＩＣカードとの間でデータのやり取りを行なうプログラムである。サービス提供プログラムは、図１で説明した公証サービス（前準備の処理も含む）を提供する際の動作全体を制御するプログラムである。通信プログラムは、通信網１８０を介して本端末３００と他の端末との通信を行なうプログラムである。暗号プログラムは、通信網１８０を介して他の端末と各種情報をやり取りする際に暗号通信を行なうプログラムである。

【００５９】リーダライタ３２０は、ＣＰＵ３３１、リーダライタ制御プログラム領域３３２、端末インタフェース３３３、およびＩＣカードインタフェース３３４を備えている。これら各部は、バス３３０によって相互に接続されている。ＣＰＵ３３１は、このリーダライタ３２０の動作（リーダライタ３２０に挿入されたＩＣカード１２０と端末３００との間のデータのやり取りに係る各種の動作）の制御を行なうＣＰＵである。ＣＰＵ３３１が実行するリーダライタ制御プログラムは、リーダライタ制御プログラム領域３３２に格納されている。端末インタフェース３３３は、端末３００との間でデータのやり取りを行なうためのインタフェースである。ＩＣカードインタフェース３３４は、このリーダライタ３２０に挿入されたＩＣカードとの間でデータのやり取りを行なうためのインタフェースである。

【００６０】図４は、サービス享受装置１４０の内部構成図である。サービス享受装置１４１も同じ構成である。サービス享受装置１４０は、図３で説明したサービス提供装置１３０とほぼ同じ構成であるので、説明は省略する。図３の各部に付された３００番台の番号を４００番台に読み替えればよい。ただし、図３のサービス提供装置１３０は公証サービスを提供する側の装置であるので領域３１６ｂにはサービス提供プログラムが格納されているが、図４のサービス享受装置１４０は公証サービスを享受する側の装置であるので領域４１６ｂにはサービス享受プログラムが格納されている。サービス享受プログラムは、図１で説明した公証サービス（前準備の処理も含む）を享受する際の動作全体を制御するプログラムである。

【００６１】図５は、図２で説明したＩＣカード１２０のデータ記憶領域２０３ｅの内容を示すブロック図であ

る。データ記憶領域２０３ｅは、外部出力禁止領域５００と、外部出力許可領域５１０と、ワーク領域５２０とからなる。外部出力禁止領域５００に格納されているデータは、ＩＣカード１２０の内部だけで使用するデータであり、ＩＣカード１２０の外部への出力は禁止される。外部出力許可領域５１０に格納されているデータは、ＩＣカード１２０の外部へ出力することができる。ワーク領域５２０は、ＩＣカード１２０のＣＰＵ２０２が演算実行の際に使用するワーク領域である。

【００６２】外部出力禁止領域５００には、秘密鍵５０１とユーザＩＤ５０２とパスワードチェック用データ５０３が格納される。秘密鍵５０１は、このＩＣカード１２０の正当な使用者が作成して設定する当該使用者の秘密鍵である。ユーザＩＤ５０２は、このＩＣカード１２０の正当な使用者の識別子である。パスワードチェック用データ５０３は、ユーザがこのＩＣカードを使用するときに入力するパスワードが正当な使用者のパスワードであるか否かをチェックするために用いるデータである。パスワードチェック用データ５０３は、パスワードそのものではなく、パスワードを何らかの一方向性の関数に通した値とする。

【００６３】外部出力許可領域５１０には、公開鍵５１１と自証明書５１２と認証機関証明書５１３とＩＣカード番号５１４とが格納される。公開鍵５１１は、このＩＣカード１２０の正当な使用者が作成して設定する当該使用者の公開鍵（上記秘密鍵５０１と対のもの）である。自証明書５１２は、認証機関１７０に発行してもらったこのＩＣカード１２０の正当な使用者（自分）の証明書である。自証明書５１２には、証明内容と認証機関１７０の署名とが含まれている。証明内容とは、このＩＣカード１２０の正当な使用者の公開鍵と他の幾つかの情報からなる。認証機関１７０の署名は、上記証明内容を一方向関数で圧縮した圧縮子を認証機関１７０の秘密鍵で暗号化し偽造不可能な形にしたものである。認証機関証明書５１３は、契約の相手方の証明書により相手方を認証する際に、認証機関１７０の署名の正当性を確認するための証明書（認証機関１７０の公開鍵）である。ＩＣカード番号５１４は、他のＩＣカードと区別するためのＩＣカード固有の番号である。

【００６４】上記ＩＣカード１２０内の各データのうち、認証機関１７０がＩＣカード１２０を発行するときに格納済みのデータは、ユーザＩＤ５０２、パスワードチェック用データ５０３、認証機関証明書５１３、およびＩＣカード番号５１４である。なお、ＩＣカード発行時にパスワードチェック用データ５０３に設定されているデータは、認証機関１７０が設定した仮パスワードに対応するデータであり、ユーザはカードを受取った後に自分でパスワードを変更する（パスワードチェック用データ５０３はパスワードの変更に伴って変更される）ことは可能である。

【００６５】図６は、図１で説明したシステムにおいて、サービス提供者１００が認証機関１７０よりＩＣカード１２１を発行してもらう手順を示す流れ図である。同図において、「サービス提供者１００」と記載された下側に並べたブロックはサービス提供者１００が行なう動作、「認証機関１７０」と記載された下側に並べたブロックは認証機関１７０が行なう動作を示す。

【００６６】サービス提供者１００は、ステップ６００でＩＣカード申込書を作成し、ステップ６０１でＩＣカード申込書を認証機関１７０に送付する。認証機関１７０は、ステップ６０２でそのＩＣカード申込書を受付け、ステップ６０３でＩＣカード申込書を送付してきた者の身元審査を行なう。身元が確認されたら、ステップ６０４でユーザ管理情報を更新し、ステップ６０５でＩＣカード１２１をサービス提供者１００に送付する。サービス提供者１００は、ステップ６０６で、ＩＣカード１２１を受け取る。

【００６７】なお、ユーザ管理情報とは、認証機関１７０がＩＣカードや証明書を発行したユーザについて管理する各種の情報のことである。また、認証機関１７０は、図５で説明したＩＣカード１２１中のデータのうち、ユーザＩＤ５０２にはユーザがＩＣカード申込書に記載したＩＤ（認証機関側でＩＤを付けることにしてもよい）を設定し、パスワードチェック用データ５０３には仮のパスワードを設定し、認証機関証明書５１３には当該認証機関１７０の公開鍵を設定し、ＩＣカード番号５１４には当該ＩＣカードの番号を設定して、ユーザに送付する。

【００６８】図６ではサービス提供者１００が認証機関１７０からＩＣカード１２１を発行してもらう手順を説明したが、サービス享受者１１０，１１１が認証機関１７０からＩＣカード１２２，１２３を発行してもらう手順も同様である。

【００６９】図７は、第１の実施の形態において、サービス提供者１００が、自ＩＣカード１２１とサービス提供装置１３０とを用いて、オンラインで認証機関１７０より証明書１５３を発行してもらう手順を示す流れ図である。同図において、「ＩＣカード１２１」と記載された下側に並べたブロックは、ＩＣカード１２１内のＣＰＵ２０２がメモリ２０３内のプログラム（図２）を実行することによる動作であり、特に、全体の流れの制御はＩＣカード制御プログラム（２０３ｂ）で、サービス提供装置１３０の端末３００との間のデータの送受信は端末・ＩＣカード間データ送受信プログラム（２０３ａ）で、秘密鍵と公開鍵の生成は暗号鍵生成プログラム（２０３ｃ）で、それぞれ、行なう。「サービス提供装置１３０」と記載された下側に並べたブロックは、サービス提供装置１３０の端末３００内のＣＰＵ３１４がメモリ３１６内のプログラム（図３）を実行することによる動作であり、特に、全体の流れの制御はサービス提供プロ

グラム（316b）で、ICカード121との間のデータの送受信は端末・ICカード間データ送受信プログラム（316a）で、認証機関170の端末との間でメッセージの送受信（暗号通信）を行なう際の該メッセージの暗号化と復号化は暗号プログラム（316d）で、認証機関170の端末との間のメッセージの送受信は通信プログラム（316c）で、それぞれ、行なう。「認証機関170」と記載された下側に並べたブロックは、認証機関170に備えられた証明書の発行業務を行なう端末における動作を示す。

【0070】サービス提供者100が、サービス提供装置130に接続されているリーダライタ320に自分のICカード121を挿入し、所定の操作を行なうことで図7の手順が開始する。まず、ステップ700で、ICカード121はサービス提供者100からの指示に基づいて秘密鍵および公開鍵を生成し、データ記憶領域203e（図5）内に秘密鍵501および公開鍵511として格納する。次に、ステップ701でICカード番号514と生成した公開鍵511とをサービス提供装置130に送信する。

【0071】サービス提供装置130は、ステップ702で、ICカード番号514と公開鍵511を受信する。次に、ステップ703で証明書要求メッセージ（ICカード番号514、公開鍵511、およびその他の必要な情報を含む）を作成し、ステップ704でその証明書要求メッセージを暗号化し、ステップ705でその暗号化証明書要求メッセージを認証機関170の端末に送信する。なお、上述したようにサービス提供装置130と認証機関170の端末との間では暗号通信を行なうが、そのための共通鍵の交換はステップ705に先立って行なっているものとする。

【0072】認証機関170の端末は、ステップ706で暗号化証明書要求メッセージを受信し、ステップ707で暗号化証明書要求メッセージを復号化する。次に、ステップ708で当該メッセージを送ってきた者の身元確認を行なう。身元が確認されたら、ステップ709で、受信した証明書要求メッセージ中の公開鍵などの情報を認証機関170の秘密鍵で暗号化して証明書を作成する。次に、ステップ710でその証明書を暗号化し、ステップ711でその暗号化証明書をサービス提供装置130に送信する。

【0073】サービス提供装置130は、ステップ712で、暗号化証明書を受信する。ステップ713でその暗号化証明書を復号化し、ステップ714で復号化した証明書をICカード121に送信する。ICカード121は、ステップ715で、証明書を受信し、データ記憶領域203eの自証明書512の領域（図5）に格納する。

【0074】なお、上記図7では、サービス提供者100が証明書を発行してもらう手順を説明したが、サービス享受者110，111が認証機関170から証明書を発行してもらう手順も同様である。図7において、ICカード121をICカード122または123に置き換え、サービス提供装置130をサービス享受装置140または141に置き換えて、同様の手順で行なえばよい。

【0075】図8は、上記図6および図7のICカード発行手順の変形例を示す。図6および図7では、認証機関170からICカードを発行してもらい、ICカードの所有者が自ら鍵生成を行なうとともに、図7の手順でオンラインで証明書を発行してもらうようにしているが、図8のようにして、始めから鍵や証明書が格納されたICカードを発行してもらうようにしてもよい。

【0076】図8の手順では、サービス提供者100は、ステップ800でICカード申込書を作成し、ステップ801でICカード申込書を認証機関170にオフラインで送付する。認証機関170では、ステップ802でICカード申込書を受付け、ステップ803で身元審査を行なう。身元が確認されたら、認証機関170の端末を用いて、ステップ804で、ICカード121内で秘密鍵および公開鍵を生成し、データ記憶領域203e（図5）内に秘密鍵501および公開鍵511として格納する。またステップ805で、ICカード121は、生成した公開鍵を認証機関170の端末に送信する。認証機関170の端末では、ステップ806でICカード121から送信された公開鍵を受信し、ステップ807でその公開鍵およびその他の情報を認証機関170の秘密鍵で暗号化して証明書を作成し、ステップ808でその証明書をICカード121に送信する。ICカード121は、ステップ809で、証明書を受信し、自証明書512（図5）として格納する。認証機関170は、ステップ810でユーザ管理情報を更新し、ステップ811で作成したICカード121をサービス提供者100に送付する。サービス提供者100は、ステップ812でそのICカード121を受け取る。

【0077】なお、不図示の処理により、ICカード121には、ICカード申込者に対応するユーザID502、パスワードチェック用データ503、認証機関証明書513、およびICカード番号514が設定されているものとする。

【0078】図8の変形例によれば、認証機関170に秘密鍵が知られてしまうこととなるが、認証機関170が信頼できる機関であれば問題はなく、サービス提供者100が行なう手間が軽減できる。

【0079】図9は、第1の実施の形態において、サービス提供者100およびサービス享受者110，111の間で行なわれるオンラインでの公証サービスの手順を示す流れ図である。同図において、「サービス享受者110」および「サービス享受者111」と記載された下側に並べたブロックは、それぞれ、サービス享受者11

０，１１１が使用するサービス享受装置１４０，１４１の端末４００内のＣＰＵ４１４がメモリ４１６内のプログラム（図４）を実行することによる動作である。特に、全体の流れの制御はサービス享受プログラム（４１６ｂ）で、サービス提供装置１３０との間でデータの送受信（暗号通信）を行なう際の該データの暗号化と復号化は暗号プログラム（４１６ｄ）で、サービス提供装置１３０との間のデータの送受信は通信プログラム（４１６ｃ）で、それぞれ、行なう。「サービス提供者１００」と記載された下側に並べたブロックは、サービス提供者１００が使用するサービス提供装置１３０の端末３００内のＣＰＵ３１４がメモリ３１６内のプログラム（図３）を実行することによる動作であり、特に、全体の流れの制御はサービス提供プログラム（３１６ｂ）で、サービス享受装置１４０，１４１との間でデータの送受信（暗号通信）を行なう際の該データの暗号化と復号化は暗号プログラム（３１６ｄ）で、サービス享受装置１４０，１４１との間のデータの送受信は通信プログラム（３１６ｃ）で、それぞれ、行なう。

【００８０】まずステップ９００ａで、サービス享受者１１０は、サービス享受装置１４０により契約内容を暗号化しサービス提供装置１３０に送信する。サービス提供装置１３０は、ステップ９０１ａでその契約内容を受信して復号化する。ステップ９００ｂ，９０１ｂは、サービス享受者１１１に関して上記ステップ９００ａ，９０１ａと同じ処理を、サービス享受装置１４１とサービス提供装置１３０との間で行なうものである。次にサービス提供者１００は、ステップ９０２で、サービス享受者１１０，１１１からそれぞれ送られてきた契約内容を照合し、照合がＯＫであれば、ステップ９０３で、所定の書式で契約内容その他の情報をまとめた契約情報１６０（図１）を作成する。そして、ステップ９０４ａ，９０４ｂで、サービス提供装置１３０によりその契約情報１６０を暗号化しサービス享受装置１４０，１４１にそれぞれ送信する。

【００８１】サービス享受者１１０側では、ステップ９０５ａで、サービス享受装置１４０により契約情報１６０を受信し復号化する。サービス享受者１１０は、ステップ９０６ａでその契約情報１６０を確認し、確認ＯＫならば、ステップ９０７ａで一者署名付き契約情報１６１（図１）を作成し、ステップ９０８ａでその一者署名付き契約情報１６１を暗号化しサービス提供装置１３０に送信する。サービス提供装置１３０は、ステップ９０９ａで、その一者署名付き契約情報１６１を受信し復号化する。ステップ９０７ａの一者署名付き契約情報１６１の作成手順については、図１３で詳しく説明する。

【００８２】図１０に、ステップ９０７ａで作成した一者署名付き契約情報１６１の構成を示す。一者署名付き契約情報１６１は、契約情報１６０と付属情報１０００ａと署名１００１ａとからなる。付属情報１０００ａは、サービス享受者１１０が署名した日時やこの契約に関連する者の名称などこの契約に付随する情報、および署名１００１ａを確認するために必要なサービス享受者１１０の証明書や認証機関の証明書からなる。署名１００１ａは、契約情報１６０と付属情報１０００ａとをこの順に連結したデータを所定の方式で圧縮し、得られた圧縮子をサービス享受者１１０の秘密鍵で暗号化して作成する。

【００８３】再び図９に戻って、サービス享受者１１１側のステップ９０５ｂ～ステップ９０８ｂは、上述したステップ９０５ａ～９０８ａの処理をサービス享受者１１１に対して行なうものである。図１１に、サービス享受者１１１側で作成した一者署名付き契約情報１６２の構成を示す。図１０と同様の構成であるが、付属情報１０００ｂと署名１００１ｂはサービス享受者１１１に関する情報である。サービス提供装置１３０は、ステップ９０９ｂで、サービス享受者１１１側の一者署名付き契約情報１６２を受信し復号化する。

【００８４】次に、サービス提供者１００は、ステップ９１０で、サービス提供装置１３０により三者署名付き契約情報１６３を作成し外部記憶装置３４０に保管する。三者署名付き契約情報１６３の作成手順については、図１４で詳しく説明する。

【００８５】図１２に、三者署名付き契約情報１６３の構成を示す。三者署名付き契約情報１６３は、契約情報１６０と付属情報１０００ａと付属情報１０００ｂと付属情報１０００ｃと署名１００１ａと署名１００１ｂと署名１００１ｃとからなる。契約情報１６０は、一者署名付き契約情報１６１，１６２に含まれている契約情報１６０である。付属情報１０００ａと署名１００１ａは一者署名付き契約情報１６１に、付属情報１０００ｂと署名１００１ｂは一者署名付き契約情報１６２に、それぞれ含まれている情報である。付属情報１０００ｃは、サービス提供者１００が付けた付属情報である。署名１００１ｃは、契約情報１６０と付属情報１０００ａ，１０００ｂ，１０００ｃと署名１００１ａ，１００１ｂとをこの順に連結したデータを所定の方式で圧縮し、得られた圧縮子をサービス提供者１００の秘密鍵で暗号化して作成する。

【００８６】このような構成の三者署名付き契約情報１６３によれば、契約情報１６０および付属情報１０００ａ，１０００ｂ，１０００ｃにより、契約内容と契約者の名称や署名日時および公証サービス提供者の名称や署名日時などの契約に関連する各種の情報が分かる。また、署名１００１ａおよび署名１００１ｂによって、契約した２者であるサービス享受者１１０および１１１が契約情報１６０（および付属情報）に対して確かに署名したものであることが確認できる。また、署名１００１ｃにより、この契約が為されていることを公証サービス提供者１００が保証していることが確認できる。契約情

報160と付属情報1000a，1000b，1000cと署名1001a，1001b，1001cはただ連結してあるだけであるので、分離して署名1001aだけ確認したり、署名1001bだけ確認することもできる。

【0087】再び図9に戻って、ステップ910の後、ステップ911aおよび911bで、サービス提供装置130は三者署名付き契約情報163を暗号化してサービス享受装置140，141に送信する。サービス享受装置140，141は、それぞれ、ステップ912a，912bで三者署名付き契約情報163を受信し復号化する。得られた三者署名付き契約情報163は、サービス享受者110，111で保管する。

【0088】なお、上述したようにサービス提供装置130とサービス享受装置140，141との間では暗号通信を行なうが、そのための共通鍵の交換は図9の処理の前処理で行なっているものとする。

【0089】図13は、図9のステップ907aの一者署名付き契約情報161の作成の手順を示す流れ図である。同図において、「サービス享受装置140」と記載された下側に並べたブロックは、サービス享受装置140の端末400内のCPU414がメモリ416内のプログラム（図4）を実行することによる動作であり、特に、全体の流れの制御はサービス享受プログラム（416b）で、ICカード122との間のデータの送受信は端末・ICカード間データ送受信プログラム（416a）で、それぞれ、行なう。「ICカード122」と記載された下側に並べたブロックは、ICカード122内のCPU202がメモリ203内のプログラム（図2）を実行することによる動作であり、特に、全体の流れの制御はICカード制御プログラム（203b）で、サービス享受装置140の端末400との間のデータの送受信は端末・ICカード間データ送受信プログラム（203a）で、署名の生成は署名生成プログラム（203d）で、それぞれ、行なう。

【0090】まずステップ1100で、サービス享受装置140は、証明書出力要求メッセージをICカード122に送信する。ICカード122は、ステップ1101でこの証明書出力要求メッセージを受信し、ステップ1102で自証明書512および認証機関証明書513を送信する。サービス享受装置140は、ステップ1103でこれらの証明書を受信し、ステップ1104で付属情報1000aを生成する。付属情報1000aは、受信した証明書と当該契約に付随する情報（署名日時やサービス享受者110の名称など）とを所定の順序で連結して生成する。次に、ステップ1105で、契約情報160と付属情報1000aとをこの順に連結したデータを圧縮し、圧縮子を生成する。ステップ1106で、圧縮子をICカード122に送信する。

【0091】ICカード122では、ステップ1107で圧縮子を受信し、ステップ1108でその圧縮子をICカード122内の（サービス享受者110の）秘密鍵501で暗号化して署名1001aを生成する。ステップ1109で、その署名1001aをサービス享受装置140に送信する。サービス享受装置140は、ステップ1110で署名1001aを受信し、ステップ1111で契約情報160と付属情報1000aと署名1001aとをこの順に連結して、図10の一者署名付き契約情報161を生成する。

【0092】なお、ステップ907bの手順も図13と同様である。ただし、ステップ907bでは、サービス享受者111に関する図11の一者署名付き契約情報162を生成する。

【0093】図14は、図9のステップ910の三者署名付き契約情報163の作成の手順を示す流れ図である。同図において、「サービス提供装置130」と記載された下側に並べたブロックは、サービス提供装置130の端末300内のCPU314がメモリ316内のプログラム（図3）を実行することによる動作であり、特に、全体の流れの制御はサービス提供プログラム（316b）で、ICカード121との間のデータの送受信は端末・ICカード間データ送受信プログラム（316a）で、それぞれ、行なう。「ICカード121」と記載された下側に並べたブロックは、ICカード121内のCPU202がメモリ203内のプログラム（図2）を実行することによる動作であり、特に、全体の流れの制御はICカード制御プログラム（203b）で、サービス提供装置130の端末300との間のデータの送受信は端末・ICカード間データ送受信プログラム（203a）で、署名の生成は署名生成プログラム（203d）で、それぞれ、行なう。

【0094】まずステップ1200で、サービス提供装置130は、証明書出力要求メッセージをICカード121に送信する。ICカード121は、ステップ1201でこの証明書出力要求メッセージを受信し、ステップ1202で自証明書512および認証機関証明書513を送信する。サービス提供装置130は、ステップ1203でこれらの証明書を受信し、ステップ1204で付属情報1000cを生成する。付属情報1000cは、受信した証明書と当該契約に付随する情報（署名日時やサービス提供者100の名称など）とを所定の順序で連結して生成する。次に、ステップ1205で、契約情報160と付属情報1000aと付属情報1000bと付属情報1000cと署名1001aと署名1001bとをこの順に連結したデータを圧縮し、圧縮子を生成する。ステップ1206で、圧縮子をICカード121に送信する。

【0095】ICカード121では、ステップ1207で圧縮子を受信し、ステップ1208でその圧縮子をICカード121内の（サービス提供者100の）秘密鍵

５０１で暗号化して署名１００１ｃを生成する。ステップ１２０９で、その署名１００１ｃをサービス提供装置１３０に送信する。サービス提供装置１３０は、ステップ１２１０で署名１００１ｃを受信し、ステップ１２１１で契約情報１６０と付属情報１０００ａと付属情報１０００ｂと付属情報１０００ｃと署名１００１ａと署名１００１ｂと署名１００１ｃとをこの順に連結して、図１２の三者署名付き契約情報１６３を生成する。

【００９６】上述の第１の実施の形態の電子公証システムによれば、商取引などを行なう際の契約に係るオンラインでの公証サービスを実現することができる。

【００９７】次に、本発明の第２の実施の形態を説明する。第２の実施の形態のシステム構成および処理手順は、上記第１の実施の形態と共通の部分が多いので、共通部分については説明を省略し、以下では第１の実施の形態と異なる部分を中心に説明する。

【００９８】上記第１の実施の形態では、サービス享受者１１０が署名した日時は付属情報１０００ａ（図１０）に含まれ、サービス享受者１１１が署名した日時は付属情報１０００ｂ（図１１）に含まれ、サービス提供者１００が署名した日時は付属情報１０００ｃ（図１２）に含まれている。しかし、これらの日時データは、サービス享受装置１４０，１４１やサービス提供装置１３０内の内蔵時計に基づくデータであるので、該内蔵時計が誤った時間を示しているときには署名日時が大幅に狂ってしまう。また、サービス享受者などが意識的に不正な日時データを設定することも考えられる。各種の契約においてはどの時点をもって契約が有効になったかが問題になる場合があるので、日時データは正確に設定されるようにしたい。そこで、第２の実施の形態では、時刻管理機関により標準時刻を管理し、付属情報に正確な日時データが設定されるようにした。

【００９９】図１５は、第２の実施の形態に係る電子公証システムのシステム図である。図１５において、図１と共通のものは同じ番号を付し、説明を省略する。図１５が図１と異なるのは、ＩＣカード１２０～１２３の代わりに内蔵時計を有するＩＣカード１３００～１３０３を用いている点と、時刻管理機関１３１０が設けられ標準時刻の管理を行なっている点である。これにより、ＩＣカード内で署名を生成する際にＩＣカード内の内蔵時計を時刻管理機関１３１０の標準時刻に基づいて調整し、調整した内蔵時計の標準時刻に基づいて付属情報の日時データを設定するようにしている。

【０１００】図１６は、図１５のシステムで用いるＩＣカード１３００（１３０１～１３０３）の内部構成図である。ＩＣカード１３００は、図２のＩＣカード１２０とほぼ同様の構成であるが、内蔵時計１４００を備えている。また、図２のＩＣカード制御プログラムの代わりに、別の処理手順のＩＣカード制御プログラムが、メモリ１４０１の領域１４０２に格納されている。

【０１０１】第２の実施の形態において、ＩＣカード発行の手順、認証機関１７０より証明書１５３～１５５を発行してもらう手順、および公証サービスの手順は、図６～図９と同じである。署名付き契約情報１６１～１６３の構成は、基本的に図１０～図１２と同様であるが、各「署名」の直前に「標準時刻」が新たに挿入される点が異なる。

【０１０２】図１７は、第２の実施の形態において図９のステップ９０７ａで実行される一者署名付き契約情報の作成の手順を示す流れ図である。ステップ１１００～１１０７の処理は、第１の実施の形態の図１３のステップ１１００～１１０７と同じである。第２の実施の形態では、ステップ１１０７の後、ステップ１５００でＩＣカード１３０２からサービス享受装置１４０に標準時刻要求メッセージを送信する。サービス享受装置１４０では、ステップ１５０１でその標準時刻要求メッセージを受信し、ステップ１５０２で標準時刻を取得する。標準時刻の取得は、図１５に示した時刻管理機関１３１０にオンラインで標準時刻要求メッセージを送信し、時刻管理機関１３１０から返送される標準時刻を受信することにより取得する。取得した標準時刻は、ステップ１５０３で、サービス享受装置１４０からＩＣカード１３０２に送信する。ＩＣカード１３０２では、ステップ１５０４でその標準時刻を受信し、受信した標準時刻に応じて内蔵時計１４００を調整する。

【０１０３】次にＩＣカード１３０２は、ステップ１１０８で、圧縮子（ステップ１１０７で受信してあるデータ）に内蔵時計１４００の標準時刻（この時点の時刻値であり、以下では標準時刻ａと呼ぶ）をこの順に連結したデータをＩＣカード１３０２内の（サービス享受者１１０の）秘密鍵５０１で暗号化して署名１００１ａを生成する。ステップ１１０９で、標準時刻ａと生成した署名１００１ａとをサービス享受装置１４０に送信する。サービス享受装置１４０は、ステップ１１１０で標準時刻ａと署名１００１ａを受信し、ステップ１１１１で契約情報１６０と付属情報１０００ａと標準時刻ａと署名１００１ａとをこの順に連結して、一者署名付き契約情報１６１を生成する。

【０１０４】なお、第２の実施の形態における図９のステップ９０７ｂの手順も図１７と同様である。ただし、ステップ９０７ｂでは、サービス享受者１１１に関する一者署名付き契約情報１６２を生成する。一者署名付き契約情報１６２は、契約情報１６０と付属情報１０００ｂと標準時刻ｂと署名１００１ｂとをこの順に連結したデータである。標準時刻ｂとは、サービス享受者１１１に関する図１７の処理のステップ１１０８で署名生成したときに用いた標準時刻の時刻値である。

【０１０５】図１８は、第２の実施の形態における図９のステップ９１０の三者署名付き契約情報の作成の手順を示す流れ図である。ステップ１２００～１２０７の処

理は、第1の実施の形態の図14のステップ1200～1207と同じである。第2の実施の形態では、ステップ1207の後、ステップ1600でICカード1301からサービス提供装置130に標準時刻要求メッセージを送信する。サービス提供装置130では、ステップ1601でその標準時刻要求メッセージを受信し、ステップ1602で標準時刻を取得する。標準時刻の取得は、図15に示した時刻管理機関1310にオンラインで標準時刻要求メッセージを送信し、時刻管理機関1310から返送される標準時刻を受信することにより取得する。取得した標準時刻は、ステップ1603で、サービス提供装置130からICカード1301に送信する。ICカード1301では、ステップ1604でその標準時刻を受信し、受信した標準時刻に応じて内蔵時計1400を調整する。

【0106】次にICカード1301は、ステップ1208で、圧縮子（ステップ1207で受信してあるデータ）に内蔵時計1400の標準時刻（この時点の時刻値であり、以下では標準時刻cと呼ぶ）をこの順に連結したデータをICカード1301内の（サービス提供者100の）秘密鍵501で暗号化して署名1001cを生成する。ステップ1209で、標準時刻cと生成した署名1001cとをサービス提供装置130に送信する。サービス提供装置130は、ステップ1210で標準時刻cと署名1001cを受信し、ステップ1211で契約情報160と付属情報1000aと付属情報1000bと付属情報1000cと標準時刻aと署名1001aと標準時刻bと署名1001bと標準時刻cと署名1001cとをこの順に連結して、三者署名付き契約情報163を生成する。

【0107】図19は、図18のステップ1602でサービス提供装置130が標準時刻を取得する手順を示す。図17のステップ1502の標準時刻の取得手順も同様である。まずステップ1700で、サービス提供装置130が時刻管理機関1310に標準時刻要求メッセージを送信する。時刻管理機関1310は、ステップ1701で標準時刻要求メッセージを受信し、ステップ1702で標準時刻を送信する。サービス提供装置130は、ステップ1703で標準時刻を受信する。なお、サービス提供装置130やサービス享受装置140，141と時刻管理機関1310との間の通信は、サービス提供装置130、サービス享受装置140，141、および認証機関170のそれぞれの間の通信と同様に、暗号通信で行なうものとする。

【0108】上述の第2の実施の形態の電子公証システムによれば、時刻管理機関1310により管理されている標準時刻を用いて正確な署名日時を契約情報に含めることができるので、契約が成立した時点が明確になり、後に契約の成立時点がいつか問題になったときに対処できる。

【0109】なお、上記第2の実施の形態では、標準時刻a，b，cは付属情報とは別に保持したが、付属情報に含める形式としてもよい。そのためには、付属情報の生成ステップの前で標準時刻を取得し、取得した標準時刻を含めて付属情報を生成するようにすればよい。また、ICカード1300は内蔵時計1400を備えるものとしたが、受信した標準時刻の値をそのまま用いるようにして内蔵時計1400を省略することもできる。

【0110】次に、本発明の第3の実施の形態を説明する。第3の実施の形態のシステム構成および処理手順は、上記第2の実施の形態と共通の部分が多いので、共通部分の説明は省略し、以下では第2の実施の形態と異なる部分を中心に説明する。

【0111】上記第2の実施の形態では、時刻管理機関1310により管理されている標準時刻でICカード1301～1303内の内蔵時計1400を調整し、その標準時刻で署名した日時を正確に記録できるようにした。しかし、ICカード1301～1303内の内蔵時計1400の調整は、基本的に、サービス提供装置130やサービス享受装置140，141を介して行なわれるものである。したがって、サービス提供装置130やサービス享受装置140，141を改造することにより、標準時刻が改変されるおそれがないとはいえない。そこで、第3の実施の形態では、サービス提供装置130やサービス享受装置140，141を介することなく、ICカード内の内蔵時計の調整ができるようにした。

【0112】図20は、第3の実施の形態に係る電子公証システムのシステム図である。図20において、図15と共通のものは同じ番号を付し、説明を省略する。図20が図15と異なるのは、ICカード1300～1303の代わりに内部に無線受信装置を備えたICカード1800～1803を用いている点である。また、不図示であるが、時刻管理機関1310からの標準時刻の送出は無線送信で行ない、直接各ICカード1800～1803で無線受信により標準時刻を取得して内蔵時計の調整を行なうようになっている。

【0113】図21は、図20のシステムで用いるICカード1800（1800～1803）の内部構成図である。ICカード1800は、図16のICカード1300とほぼ同様の構成であるが、内蔵時計1400に加えて無線受信装置1900を備えている。また、図16のICカード制御プログラムの代わりに、別の処理手順のICカード制御プログラムが、メモリ203の領域1901に格納されている。

【0114】第3の実施の形態において、ICカード発行の手順、認証機関170より証明書153～155を発行してもらう手順、公証サービスの手順、および署名付き契約情報161～163の構成は、上述の第2の実施の形態と同じである。

【０１１５】図２２は、第３の実施の形態において図９のステップ９０７ａで実行される一者署名付き契約情報の作成の手順を示す流れ図である。ステップ１１００～１１０７の処理は、第２の実施の形態の図１７のステップ１１００～１１０７と同じである。第３の実施の形態では、ステップ１１０７の後、ステップ２００１でＩＣカード１８０２内の無線受信装置１９００により標準時刻を受信する。時刻管理機関１３１０では、無線送信装置により標準時刻を常時送信しているので、ステップ２０００で送信されている標準時刻をステップ２００１で受信すればよい。ＩＣカード１８０２は、ステップ２００２で、受信した標準時刻に応じて内蔵時計１４００を調整する。これ以降のステップ１１０８～１１１１の処理は、第２の実施の形態の図１７のステップ１１０８～１１１１と同じである。以上により、サービス享受者１１０に関する一者署名付き契約情報１６１を生成する。なお、第３の実施の形態における図９のステップ９０７ｂの手順も図２２と同様である。ただし、ステップ９０７ｂでは、サービス享受者１１１に関する一者署名付き契約情報１６２を生成する。

【０１１６】図２３は、第３の実施の形態における図９のステップ９１０の三者署名付き契約情報の作成の手順を示す流れ図である。ステップ１２００～１２０７の処理は、第２の実施の形態の図１８のステップ１２００～１２０７と同じである。第３の実施の形態では、ステップ１２０７の後、ステップ２１０１でＩＣカード１８０１内の無線受信装置１９００により標準時刻を受信する。時刻管理機関１３１０では、無線送信装置により標準時刻を常時送信しているので、ステップ２１００で送信されている標準時刻をステップ２１０１で受信すればよい。ＩＣカード１８０１は、ステップ２１０２で、受信した標準時刻に応じて内蔵時計１４００を調整する。ステップ１２０８～１２１１の処理は、第２の実施の形態の図１８のステップ１２０８～１２１１と同じである。以上により、三者署名付き契約情報１６３を生成する。

【０１１７】上述の第３の実施の形態の電子公証システムによれば、時刻管理機関１３１０により管理されている標準時刻は、サービス提供装置１３０やサービス享受装置１４０，１４１を介することなく、直接、無線で時刻管理機関１３１０から各ＩＣカード１８０１～１８０３に送られる。したがって、サービス提供装置１３０やサービス享受装置１４０，１４１において日時に改変を施す不正ができなくなり、正確な署名日時を契約情報に含めることができるようになる。

【０１１８】次に、本発明の第４の実施の形態を説明する。第４の実施の形態のシステム構成および処理手順は、上記第１の実施の形態と共通の部分が多いので、共通部分の説明は省略し、以下では第１の実施の形態と異なる部分を中心に説明する。

【０１１９】図２４は、第４の実施の形態に係る電子公証システムのシステム図である。図２４において、図１と共通のものは同じ番号を付し、説明を省略する。図２４のが図１と異なるのは、ＩＣカード発行機関１８０が存在せず、ＩＣカード１２０～１２３の代わりにフロッピーディスク２２２０～２２２２を用いている点である。なお、フロッピーディスク以外の記憶媒体を用いることも可能である。

【０１２０】図２５は、第４の実施の形態のシステムにおけるサービス提供装置２２００の内部構成図である。同図のサービス提供装置２２００は、図３に示した第１の実施の形態のサービス提供装置１３０とほぼ同じ構成であるが、リーダライタとそのインターフェースを備えていない点、および端末２３００内のメモリ２３１０内の構成が異なる。メモリ２３１０には、サービス提供プログラムが記憶されている領域３１６ｂ、通信プログラムが記憶されている領域３１６ｃ、暗号プログラムが記憶されている領域３１６ｄ、各種のワーク用データが記憶されるデータ記憶領域３１６ｅ、暗号鍵生成プログラムが記憶されている領域２３１１、および署名生成プログラムが記憶されている領域２３１２が設けられている。領域２３１１，２３１２に記憶されている暗号鍵生成プログラムと署名生成プログラムは、第１の実施の形態のＩＣカード１２０内に備えられている暗号鍵生成プログラムと署名生成プログラムと同様の機能を持つものであるが、第４の実施の形態ではＩＣカードの代わりにフロッピーディスクを用いるので、これらのプログラムはサービス提供装置２２００内に備えられている。

【０１２１】図２６は、第４の実施の形態のシステムにおけるサービス享受装置２２１０の内部構成図である。サービス享受装置２２１１も同じ構成である。サービス享受装置２２１０は、図２５で説明したサービス提供装置２２００とほぼ同じ構成であるので、説明は省略する。図２５の各部に付された３００番台および２３００番台の番号を４００番台および２４００番台に読み替えればよい。ただし、図２５のサービス提供装置２２００は公証サービスを提供する側の装置であるので領域３１６ｂにはサービス提供プログラムが格納されているが、図２６のサービス享受装置２２１０は公証サービスを享受する側の装置であるので領域４１６ｂにはサービス享受プログラムが格納されている。

【０１２２】図２７は、図２４のシステム図におけるフロッピーディスク２２２０の内容を示すブロック図である。フロッピーディスク２２２０には、暗号化秘密鍵２５００、ユーザＩＤ２５０１、パスワードチェック用データ２５０２、暗号化公開鍵２５０３、暗号化自証明書２５０４、認証機関証明書２５０５、およびフロッピーディスク番号２５０６が格納される。これらの情報は、第１の実施の形態の図５で説明したＩＣカード１２０のデータ記憶領域２０３ｅに格納される情報と同様のもの

である。ただし、フロッピーディスクはＩＣカードに比較して簡単に情報が読み出せるので、秘密鍵２５００と公開鍵２５０３と自証明書２５０４は、このフロッピーディスク２２２０の正当なユーザのパスワードを鍵として暗号化されている。すなわち、このフロッピーディスク２２２０を使用する際には、以下の手順で行なうことが要求される。

【０１２３】このフロッピーディスク２２２０を使用するとき、ユーザは、ユーザＩＤとパスワードの入力を装置から要求される。入力されたユーザＩＤはユーザＩＤ２５０１と照合され、入力されたパスワードは所定の一方向性の圧縮関数を通してパスワードチェック用データ２５０２と照合される。照合の結果、正当なユーザであると確認されたら、そのパスワードを端末側のワーク領域に記憶しておく。この後は、暗号化秘密鍵２５００、暗号化公開鍵２５０３、または暗号化自証明書２５０４を必要に応じて読み出したとき、記憶してあるパスワードでこれらの情報を復号化し、秘密鍵、公開鍵、および自証明書を得る。

【０１２４】上記ではフロッピーディスク２２２０について説明したが、フロッピーディスク２２２１，２２２２も同様のものである。

【０１２５】図２８は、第４の実施の形態において、サービス提供者１００が認証機関１７０よりフロッピーディスク２２２０を発行してもらう手順を示す流れ図である。同図において、「サービス提供者１００」と記載された下側に並べたブロックはサービス提供者１００が行なう動作、「認証機関１７０」と記載された下側に並べたブロックは認証機関１７０が行なう動作を示す。

【０１２６】サービス提供者１００は、ステップ２６００でフロッピーディスク申込書を作成し、ステップ２６０１でフロッピーディスク申込書を認証機関１７０に送付する。認証機関１７０は、ステップ２６０２でそのフロッピーディスク申込書を受付け、ステップ６０３でフロッピーディスク申込書を送付してきた者の身元審査を行なう。身元が確認されたら、ステップ６０４でユーザ管理情報を更新し、ステップ２６０３でフロッピーディスク２２２０をサービス提供者１００に送付する。サービス提供者１００は、ステップ２６０６で、フロッピーディスク２２２０を受け取る。

【０１２７】なお、認証機関１７０は、図２７で説明したフロッピーディスク２２２０中のデータのうち、ユーザＩＤ２５０１にはユーザがフロッピーディスク申込書に記載したＩＤ（認証機関側でＩＤを付けることにしてもよい）を設定し、パスワードチェック用データ２５０２には仮パスワードのチェック用データを設定し、認証機関証明書２５０５には当該認証機関の公開鍵を設定し、フロッピーディスク番号２５０６には当該フロッピーディスクの番号を設定して、ユーザに送付する。

【０１２８】図２８ではサービス提供者１００が認証機関１７０からフロッピーディスク２２２０を発行してもらう手順を説明したが、サービス享受者１１０，１１１が認証機関１７０からフロッピーディスク２２２１，２２２２を発行してもらう手順も同様である。

【０１２９】図２９は、第４の実施の形態において、サービス提供者１００が、自フロッピーディスク２２２０とサービス提供装置２２００とを用いて、オンラインで認証機関１７０より証明書１５３を発行してもらう手順を示す流れ図である。同図において、「フロッピーディスク２２２０」と記載された下側に並べたブロックは、フロッピーディスク２２２０へのアクセスを示す。「サービス提供装置２２００」と記載された下側に並べたブロックは、サービス提供装置２２００の端末２３００内のＣＰＵ３１４がメモリ２３１０内のプログラム（図２５）を実行することによる動作であり、特に、全体の流れの制御はサービス提供プログラム（３１６ｂ）で、認証機関１７０の端末との間でメッセージの送受信（暗号通信）を行なう際の該メッセージの暗号化と復号化は暗号プログラム（３１６ｄ）で、認証機関１７０の端末との間のメッセージの送受信は通信プログラム（３１６ｃ）で、暗号鍵の生成は暗号鍵生成プログラム（２３１１）で、それぞれ、行なう。「認証機関１７０」と記載された下側に並べたブロックは、認証機関１７０に備えられた証明書の発行業務を行なう端末における動作を示す。

【０１３０】サービス提供者１００が、サービス提供装置２２００に自分のフロッピーディスク２２２０を挿入し、所定の操作を行なうことで図２９の手順が開始する。まずサービス提供装置２２００は、ステップ２７００でサービス提供者１００からの指示に基づいて秘密鍵および公開鍵を生成し、ステップ２７０１で秘密鍵および公開鍵をパスワードで暗号化してフロッピーディスク２２２０に書き込む。ステップ２７０２で、フロッピーディスク２２２０は、図２７に示した所定の領域２５００，２５０３に暗号化秘密鍵と暗号化公開鍵をそれぞれ格納する。

【０１３１】ステップ７０３～７１３の処理は、第１の実施の形態の図７のステップ７０３～７１３と同じ処理である。この処理により、サービス提供装置２２００は、認証機関１７０から証明書を取得する。ステップ２７０３で証明書をパスワードで暗号化し、フロッピーディスク２２２０に書き込む。フロッピーディスク２２２０は、ステップ２７０４で、暗号化証明書を図２７に示した所定の領域２５０４に格納する。

【０１３２】なお、上記図２９では、サービス提供者１００が証明書を発行してもらう手順を説明したが、サービス享受者１１０，１１１が認証機関１７０から証明書を発行してもらう手順も同様である。

【０１３３】この第４の実施の形態において、サービス提供者１００およびサービス享受者１１０，１１１の間

で行なわれるオンラインでの公証サービスの手順は、第１の実施の形態の図９で説明した手順と同様である。ただし、図９の手順では、サービス享受者１１０，１１１側で行なわれるステップ９０７ａ，９０７ｂの一者署名付き契約情報の作成、およびサービス提供者１００側で行なわれるステップ９１０の三者署名付き契約情報の作成は、図１３および図１４に示すようにＩＣカードを用いて行なっているが、第４の実施の形態ではＩＣカードの代わりにフロッピーディスクを用いるのでこれらの契約情報の作成手順は異なる。

【０１３４】図３０は、第４の実施の形態において、図９のステップ９０７ａの一者署名付き契約情報の作成の手順を示す流れ図である。サービス享受装置２２１０は、ステップ２８００で、フロッピーディスク２２２１から暗号化秘密鍵２５００と暗号化自証明書２５０４と認証機関証明書２５０５とを読み取る。読み取った暗号化秘密鍵２５００と暗号化自証明書２５０４は、パスワードで復号化しておく。次に、ステップ１１０４で、付属情報１０００ａを生成する。付属情報１０００ａは、自証明書や認証機関証明書と当該契約に付随する情報（署名日時やサービス享受者１１０の名称など）とを所定の順序で連結して生成する。次に、ステップ１１０５で、契約情報１６０と付属情報１０００ａとをこの順に連結したデータを圧縮し、圧縮子を生成する。ステップ２８０１では、作成した圧縮子を秘密鍵で暗号化して署名１００１ａを作成する。ステップ１１１１で、契約情報１６０と付属情報１０００ａと署名１００１ａとをこの順に連結して、図１０の一者署名付き契約情報１６１を生成する。

【０１３５】なお、ステップ９０７ｂの手順も図３０と同様である。ただし、ステップ９０７ｂでは、サービス享受者１１１に関する図１１の一者署名付き契約情報１６２を生成する。

【０１３６】図３１は、第４の実施の形態において、図９のステップ９１０の三者署名付き契約情報の作成の手順を示す流れ図である。サービス提供装置２２００は、まずステップ２９００で、フロッピーディスク２２２０から暗号化秘密鍵２５００と暗号化自証明書２５０４と認証機関証明書２５０５とを読み取る。読み取った暗号化秘密鍵２５００と暗号化自証明書２５０４は、パスワードで復号化しておく。次に、ステップ１２０４で、付属情報１０００ｃを生成する。付属情報１０００ｃは、自証明書や認証機関証明書と当該契約に付随する情報（署名日時やサービス提供者１００の名称など）とを所定の順序で連結して生成する。次に、ステップ１２０５で、契約情報１６０と付属情報１０００ａと付属情報１０００ｂと付属情報１０００ｃと署名１００１ａと署名１００１ｂとをこの順に連結したデータを圧縮し、圧縮子を生成する。ステップ２９０１では、作成した圧縮子を秘密鍵で暗号化して署名１００１ｃを作成する。ステップ１２１１で、契約情報１６０と付属情報１０００ａと付属情報１０００ｂと付属情報１０００ｃと署名１００１ａと署名１００１ｂと署名１００１ｃとをこの順に連結して、図１２の三者署名付き契約情報１６３を生成する。

【０１３７】上述の第４の実施の形態によれば、安価なフロッピーディスクを用いてオンラインでの公証サービスを実現することができる。

【０１３８】次に、本発明の第５の実施の形態を説明する。上述の第１～第３の実施の形態ではＩＣカードを用いた公証サービスのシステムを説明したが、第５の実施の形態はそれらの変形例と見ることもできるものであるので、共通部分の説明は省略し、異なる部分のみ説明する。。

【０１３９】第５の実施の形態では、各者の鍵と証明書は、一定期間で変更することを前提とする。これらを一定期間で変更していくことにより、鍵の安全性を高めることができる。しかし、以前に使用していた鍵や証明書を捨ててしまうと、その捨てた鍵を用いて生成した署名を確認・認証できなくなるという不都合がある。そこで、第５の実施の形態では、ＩＣカードに、以前に使用した鍵と証明書を保存しておくようにしている。

【０１４０】図３２は、本発明の第５の実施の形態に係るＩＣカードのデータ記憶領域３０００の内容を示す。同図において、図５と同じ情報および領域には同じ番号を付して説明を省略する。このＩＣカードでは、署名履歴３０２２を記憶する領域を設けておき、署名したときには、どの鍵と証明書を用いて何時署名したかの履歴を保存するようにする。そして、秘密鍵５０１、公開鍵５１１、自証明書５１２、および認証機関証明書５１３を新たなものに変更したときには、署名履歴３０２２を参照して、それまで使用していた秘密鍵５０１、公開鍵５１１、自証明書５１２、および認証機関証明書５１３を保持しておく必要があったら（それらの鍵や証明書での署名を確認する必要が生じると思われるような場合）、領域３０１１，３０２１に退避する。

【０１４１】第５の実施の形態のＩＣカードによれば、以前に使用していた鍵や証明書を保存しているので、以前の鍵による署名の確認・認証が行なえる。また、署名履歴３０２２を参照して、その鍵で署名した文書を確認・認証することがなくなったことを確認したら、以前に使用した鍵および証明書を削除すればよい。

【０１４２】次に、この発明の第６の実施の形態を説明する。上述の各実施の形態のシステムでは、一つの認証機関１７０がＩＣカードやフロッピーディスクの発行および証明書の発行業務を行なっている。これに対し、第６の実施の形態のシステムは、認証機関を、個人を認証する個人認証局と会員を認証する会員認証局とに分けた点を特徴とするものである。

【０１４３】図３３は、第６の実施の形態のシステム構

成図を示す。ネットワークを介して、会員認証局の端末３３１０、個人認証局の端末３３２０、会員Ａの端末３３３０、および会員Ｂの端末３３４０が接続されている。ネットワークは、インターネットなどのオープンなネットワーク環境である。

【０１４４】個人認証局は、個人の公開鍵が真正な本人のものであることを証明し、それを証明する証明書（個人認証書）の発行、保管、および失効の処理を行なう機関である。また、個人認証局は、個人認証書の有効性についての問い合わせに対して応答する。個人認証局への登録は、住民記録に相当するようなものであり、例えば公的機関での運営が想定される。

【０１４５】図３３において、個人認証局の端末３３２０は、制御モジュール３３２１、個人登録モジュール３３２２、個人認証モジュール３３２３、個人登録抹消モジュール３３２４、および個人認証書データベース３３２５を備えている。制御モジュール３３２１は、申請者の申込みに基づき処理を振り分ける処理を行なう。個人登録モジュール３３２２は、申請者の申込みに基づき個人の真正さを審査し、個人認証書を発行する処理を行なう。個人認証モジュール３３２３は、申請者の依頼に基づき、個人認証書の有効性を確認し、その結果を申請者に通知する処理を行なう。個人登録抹消モジュール３３２４は、申請者の依頼に基づき個人登録を抹消する処理を行なう。個人認証書データベース３３２５は、各個人の公開鍵その他の情報を保管するデータベースである。

【０１４６】会員認証局は、ある特定の団体等の会員資格を有する個人の公開鍵が会員資格を有する本人のものであることを証明し、それを証明する会員証の発行、保管、および失効の処理を行なう機関である。また、会員認証局は、会員証の有効性についての問い合わせに対して応答する。上述の個人認証局が住民登録を行なう公的機関のようなものであるのに対し、会員認証局は、例えばクレジットカードの会員であることを証明するような機関である。

【０１４７】図３３において、会員認証局の端末３３１０は、制御モジュール３３１１、会員登録モジュール３３１２、会員認証モジュール３３１３、会員登録抹消モジュール３３１４、および会員証データベース３３１５を備えている。制御モジュール３３１１は、申請者のネットワークを介した申込みに基づいて処理を振り分ける処理を行なう。会員登録モジュール３３１２は、申請者の申込みに基づき会員資格を審査し、会員資格があると認めた者に会員証を発行する処理を行なう。会員認証モジュール３３１３は、申請者の依頼に基づき会員証の有効性を確認し、その結果を申請者に通知する処理を行なう。会員登録抹消モジュール３３１４は、申請者の依頼に基づき、会員登録を抹消する処理を行なう。会員証データベース３３１５は、会員資格を有する各個人の公開鍵その他の情報を保管するデータベースである。

【０１４８】会員Ａの端末３３３０は、情報交換モジュール３３３１、およびＩＣカード入出力モジュール３３３２を備えている。情報交換モジュール３３３１は、ネットワークを介して他の端末と情報をやり取りする各種の処理を行なう。ＩＣカード入出力モジュール３３３２は、個人認証局や会員認証局から発行されたＩＣカードとの間で各種の情報を入出力するためのモジュールである。会員Ｂの端末３３４０は、情報交換モジュール３３４１およびＩＣカード入出力モジュール３３４２を備えている。これらは会員Ａの端末３３３０に備えられているものと同様のモジュールである。

【０１４９】図３４に、会員証データベース３３１５の内部構造を示す。会員証データベース３３１５は、各会員ごとに、会員証番号、会員名、個人認証書番号、有効期間、会員の公開鍵、および予備の情報を格納するデータベースである。有効期間は、開始日時と終了日時とからなる。会員の公開鍵は、鍵のアルゴリズム、および鍵のビット列からなる。図示しないが、個人認証局の端末３３２０に備えられている個人認証書データベース３３２５も同様の構造を有するものであり、各個人ごとに、個人名、個人認証書番号、有効期間、個人の公開鍵、および予備の情報を格納している。

【０１５０】図３５は、図３３のシステムによる会員登録の手順を示す流れ図である。まず申込者は、個人認証局に対して個人認証書の発行・送付依頼を行なう。個人認証局は、登録の申請者が確かにその者であるか否か身元を審査し、身元が確認できたら個人認証書を発行・送付する。個人認証書は、住民登録の証明書に相当するようなものであり、具体的には、その個人の公開鍵とその公開鍵がその個人のものであることを証明する個人認証局の証明書とを含むディジタルデータである。通常、個人認証局での身元審査は対面審査によると考えられるので、申込者からの個人認証書の発行・送付依頼や個人認証局からの個人認証書の送付は、申込者が個人認証局に出向いて行なう。ただし、身元審査を行なう手段があれば、ネットワークを介してオンラインで行なってもよい。個人認証書はディジタルデータであるので、個人認証書を受け取った個人は、ＩＣカードやフロッピーディスクなど任意の記憶装置に個人認証書を格納して管理する。ここでは、ＩＣカードに個人認証書を格納して管理するものとする。

【０１５１】次に申込者は、以下の手順で会員登録を行なう。以下、会員証登録の通知までの手順は、特に指摘した処理を除き、ネットワークを介してオンラインで行なうものである。

【０１５２】まず、申込者が申込者の端末（３３３０や３３４０）で会員登録申込書送付依頼を指示する操作を行なうと、申込者の端末は、会員認証局の端末３３１０に対して会員登録申込書の送付依頼を行なう。会員認証局の端末３３１０は、その依頼に応じて会員登録申込書

を送付する。会員登録申込書を受信した申込者の端末は、その会員登録申込書をディスプレイに表示する。申込者がディスプレイ上で会員登録申込書に所定の事項を書き込み、その会員登録申込書の送付を端末に指示すると、申込者の端末は、書き込み済みの会員登録申込書に個人認証書を添付して、会員認証局の端末３３１０に送付する。会員認証局の端末３３１０は、その申込書と個人認証書を受け取ったら、申込受付の応答を申込者の端末に返す。

【０１５３】次に会員認証局の端末３３１０は、送付されてきた個人認証書の有効性の確認依頼を個人認証局の端末３３２０に対して行なう。個人認証局の端末３３２０は、その個人認証書の有効性を確認し、確認結果を会員認証局の端末３３１０に送付する。会員認証局の端末３３１０でその確認結果を受けたら、会員認証局は、その確認結果およびその他の情報に基づいて会員資格の審査を行ない、会員資格有りと判断されたときは、鍵生成ソフトが内蔵されているＩＣカードを申込者に郵送する。

【０１５４】申込者は、申込者の端末にそのＩＣカードを挿入してそのＩＣカード中で会員証を作成する。具体的には、会員として使用する公開鍵と秘密鍵のペアを生成し、秘密鍵はＩＣカード内の外部出力禁止領域に格納し、公開鍵はＩＣカード内の外部出力許可領域に格納するとともに、生成した公開鍵を含む申込者に関する所定の情報を所定のフォーマットでまとめたデータである会員証をＩＣカード内に作成するということである。申込者は、申込者の端末を使用して、作成した会員証に個人認証書を添付して会員認証局の端末３３１０に送付する。

【０１５５】会員認証局の端末３３１０は、送付された個人認証書の有効性の確認依頼を個人認証局の端末３３２０に対して行ない、個人認証局の端末３３２０は、その個人認証書の有効性を確認する。確認結果は会員認証局の端末３３１０に送付される。個人認証書の有効性が確認されたら、会員認証局の端末３３１０は、会員証の登録を行ない申込者に会員証登録の通知を行なう。具体的には、その申込者の公開鍵を含む会員証が確かにその者のものであることを証明する証明書を申込者に送付するということである。申込者の端末は、送られてきた証明書をＩＣカードに格納する。以上によりこの申込者の会員登録が行なわれた。

【０１５６】なお、上述の図３５の手順は、申込者が個人認証局から個人認証書を送付してもらうまでのフェーズ、申込者が会員認証局に会員登録申込書の送付依頼を出してから申込受付の応答を受領するまでのフェーズ、会員認証局が会員登録申込書を受けてからＩＣカードを申込者に郵送するまでのフェーズ、申込者がＩＣカードを受け取ってから会員証を作成し個人認証書を添付して会員認証局に送付するまでのフェーズ、および会員認証局が申込者から会員証と個人認証書の送付を受けてから会員証登録の通知を出すまでのフェーズに分かれており、これら各フェーズ間にはタイムラグがある。そのため、そのタイムラグの間に個人認証書が無効になる場合も考えられるので、会員認証局から個人認証局への個人認証書の確認は２回行なっている。ただし、個人認証書の確認を１回で済ませてもよい。その場合は、申込者がＩＣカード内で会員証を作成して会員認証局の端末３３１０に送信したら（個人認証書の添付は不要）、会員認証局の端末３３１０で、個人認証書の有効性の確認を行なうことなく、会員証の登録を行ない申込者に会員証登録の通知を行なうようにすればよい。

【０１５７】図３６は、会員登録抹消の手順を示す流れ図である。申込者が申込者の端末（３３３０や３３４０）で会員登録抹消処理を指示すると、申込者の端末は、個人認証書と会員証とを添付して会員登録の抹消の申込みを会員認証局の端末３３１０に対して送信する。会員認証局の端末３３１０は、送られてきた個人認証書の有効性の確認依頼を個人認証局の端末３３２０に対して発行する。個人認証局の端末３３２０は、その個人認証書の有効性を確認し、その確認結果を会員認証局の端末３３１０に送付する。会員認証局の端末３３１０は、その確認結果を受けて、個人認証書が有効なものであれば会員証の有効性を確認した上で、当該会員の会員登録を抹消し、会員者登録抹消の通知を申込者の端末に対して行なう。

【０１５８】以上の手順によれば、個人認証書を確認することにより本人からの登録抹消依頼であることが確認できる。これにより、個人認証書を入手した第３者が悪用しようとしたとき（会員登録を抹消しようとしたとき）、本人が個人認証局に個人認証書の紛失を届けていれば、個人認証書の有効性を確認する際に紛失したものであることが判明するので、悪用を防止することができる。同様に、会員証の確認も行なっているので、会員証を入手した第３者が悪用しようとしたとき（会員登録を抹消しようとしたとき）、本人が会員認証局に会員証の紛失を届けていれば、会員証の有効性を確認する際に紛失したものであることが判明するので、悪用を防止することができる。この例では、個人認証書と会員証は別のＩＣカードに格納しているが、個人認証書のＩＣカードを紛失したときは個人認証局に、会員証のＩＣカードを紛失したときは会員認証局に、それぞれ届け出ることになるので、何れか一方を紛失しても個人認証書の確認または会員証の確認のどちらかでチェックされ悪用は防止できる。

【０１５９】図３７は、会員Ａと会員Ｂとの間で何らかの取引を行なうとき相手を確認するための手順を示す。まず、会員Ａの端末３３３０から個人認証書と会員証の送付依頼を、会員Ｂの端末３３４０に対して送信する。この送付依頼に応じて、会員Ｂの端末３３４０は、会員

Bの個人認証書と会員証を会員Aの端末3330に送信する。会員Aの端末3330は、受信した会員Bの会員証と個人認証書とを会員認証局の端末3310に送信して、会員Bの有効性の確認依頼を行なう。これを受けて、会員認証局の端末3310は、会員Bの会員証の有効性を確認するとともに、個人認証局の端末3320に対して個人認証書の有効性の確認依頼を送信する。個人認証局の端末3320は、この依頼に基づき個人認証書の有効性を確認し、確認結果を会員認証局の端末3310に送付する。会員認証局の端末3310は、会員証の確認結果を会員Aの端末3330に通知する。

【0160】以上により、会員Aは、会員Bの会員証と個人認証書の両方の有効性を確認して、会員Bの真正性を確認することができる。会員Bが会員Aの真正性を確認するのも同様に行なえばよい。

【0161】図38は、図33の会員認証局の端末3310の制御モジュール3311の処理手順を示すフローチャートである。まずステップ3801で、会員からの依頼内容（ネットワークを介して会員の端末3330や3340から送信されてきた依頼内容）を判別し、その依頼内容に応じて分岐する。依頼内容が会員登録であるときは、ステップ3702で会員登録モジュール3312により会員登録の処理を行なう。依頼内容が会員認証であるときは、ステップ3703で会員認証モジュール3313により会員認証の処理を行なう。依頼内容が会員登録抹消であるときは、ステップ3704で会員登録抹消モジュール3314により会員登録抹消の処理を行なう。

【0162】図39は、図38のステップ3802の会員登録モジュール3312による処理手順を示すフローチャートである。このフローチャートは、図35の手順のうち、申込者が会員認証局に会員登録申込書の送付依頼を出してから会員認証局が会員資格の審査結果を出すまでの、会員認証局の端末3310が行なう処理を示すものである。まずステップ3901で、申込者の端末3330や3340から送信された会員登録申込書送付依頼を受付け、ステップ3902で、その申込者の端末へ会員登録申込書を送信する。会員登録申込書は所定フォームの電子的な文書であり、申込者はその会員登録申込書に各種の事項を書き込んだ後、その会員登録申込書と自分の個人認証書とを会員認証局の端末3310に送信してくるので、ステップ3903でそれらを受付ける。会員登録申込書と個人認証書とを受付けたら、ステップ3904で、申込者の端末に申し込み受付を応答する。

【0163】次に、会員認証局の端末3310は、ステップ3905で、個人認証局の端末3320に対し、当該申込者の個人認証書の有効性の確認を依頼する。個人認証局の端末3320は、その依頼に基づいて当該個人認証書の有効性を確認し、確認結果を会員認証局の端末3310に送信するので、会員認証局の端末3310では、ステップ3306でその確認結果を受領し、当該個人認証書が有効であるか無効であるか判別する。無効であるときは、ステップ3909で会員資格が無い旨を申込者の端末に通知し処理を終了する。当該個人認証書が有効なものであるときは、ステップ3907で会員資格を審査する。会員資格有りの場合は、ステップ3908で、会員登録を実施して良い旨を表示し処理を終了する。会員資格が無しの場合は、ステップ3909に進む。

【0164】図39の処理により会員登録を実施して良い場合は、図35で説明したように鍵生成ソフト内蔵のICカードを当該申込者に郵送する。申込者は、ICカード中で会員証を作成し、会員証に個人認証書を添付して会員認証局の端末3310に送付する。

【0165】図40は、申込者から送られてくる会員証と個人認証書を受け付けるところから会員証登録の通知を行なうまでの、会員認証局の端末3310の、処理手順を示すフローチャートである。まずステップ4001で、申込者の端末（3330や3340）から送信されてくる会員証と個人認証書を受け付ける。次にステップ4002で、個人認証局の端末3320に対し、当該個人認証書の有効性の確認を依頼する。個人認証局の端末3320は、その個人認証書の有効性を確認し、確認結果を会員認証局の端末3310に送信してくるので、会員認証局の端末3310では、ステップ4003でその確認結果を受領し、有効か無効かを判別する。当該個人認証書が有効なものであるときは、ステップ4004で会員証データベース3315に当該申込者の各種の情報を登録し、ステップ4005で申込者に会員証登録完了の旨を通知して処理を終了する。会員証登録完了の通知には、会員資格を有するこの申込者の公開鍵が確かに本人のものであることを証明する証明書（具体的には、公開鍵を含む所定の情報を会員認証局の秘密鍵で暗号化したもの）を含む会員証が含まれている。ステップ4003で当該個人認証書が無効なものであるときは、ステップ4006で、会員登録ができない旨を当該申込者に通知して処理を終了する。

【0166】図41は、図38のステップ3804の会員登録抹消モジュール3314による処理手順を示すフローチャートである。このフローチャートは、図36で会員認証局の端末3310が行なう処理を示すものである。まずステップ4101で、会員の端末（3330や3340）から送信されてくるその会員本人の個人認証書と会員証と会員登録の抹消の申込みを受け付ける。次にステップ4102で、個人認証局3320に対し、当該個人認証書の有効性の確認を依頼する。個人認証局の端末3320は、この依頼を受けて当該個人認証書の有効性を確認し確認結果を送信してくるので、会員認証局3310では、ステップ4103でその確認結果を受領し、有効か無効かを判別する。当該個人認証書が有効な

ものであるときは、ステップ４１０４で、会員証の有効性を確認した上で、会員証データベース３３１５中の当該会員の情報を無効とする。また、ステップ４１０５で当該申込者に対し会員登録抹消を通知して、処理を終了する。ステップ４１０３で当該個人認証書が無効なものであったときは、ステップ４１０６で、会員登録抹消不可の旨を当該申込者に通知して処理を終了する。

【０１６７】図４２は、図３８のステップ３８０３の会員認証モジュール３３１３による処理手順を示すフローチャートである。このフローチャートは、図３７で説明した会員認証局の端末３３１０が行なう処理である。まずステップ４２０１で、会員の端末から送信されてくる有効性を確認したい対象者の個人認証書と会員証を受け付ける。次にステップ４２０２で、会員証データベース３３１５を参照し、当該会員証の有効性を確認する。当該会員証が有効なものであるときは、ステップ４２０３で、個人認証局３３２０に対し当該個人認証書の有効性の確認を依頼する。個人認証局の端末３３２０は、その依頼を受けて個人認証書の有効性を確認し、確認結果を送信してくるので、会員認証局の端末３３１０は、ステップ４２０４でその確認結果を受領し、有効か無効かを判別する。当該個人認証書が有効なものであるときは、ステップ４２０５で、その申込者に対し会員証が有効である旨を通知して、処理を終了する。ステップ４２０４で当該個人認証書が無効なものであるときは、ステップ４２０６で、その申込者に対して会員証が無効である旨を通知し、処理を終了する。

【０１６８】以上説明した第６の実施の形態によれば、会員認証局は、会員登録処理時に個人認証局に対し個人認証書の有効性の確認を行なってもらうことにより、個人の識別を非対面で行なうことができる。住民登録に相当するような個人認証は公的機関がその役割を担うことが想定され、そこでは対面してその個人の身元確認を行なうと考えられる。一方、各種の団体などで会員登録を行なう際には、個人認証局に照会しさえすればその個人の身元確認ができるので、非対面で会員登録を行なうことができ、会員登録の処理の手間が省ける。この際、公的機関が保管すべき個人のプライバシー情報は見ることなく、会員としての審査に必要な情報のみを個人認証局から会員認証局へ送付することにより、各個人のプライバシーを侵害することなく身元確認が行なえる。また、会員ＡおよびＢ間で各種の取引を行なうときの確認は、会員証の確認と個人認証書の確認の両方を行なうようにしているので、取引を行なおうとしている相手方の真正性が確度高く確認できる。会員認証書と個人認証書とを別々のＩＣカードなどで保有しているので、どちらかを紛失したときには、会員認証局または個人認証局に届け出ておけば、悪用の可能性は少ない。

【０１６９】次に、この発明の第７の実施の形態を説明する。上記各実施の形態で説明したように各個人の公開鍵を所定の認証機関に登録して証明書を発行してもらう場合、登録の手間を軽減するため、複数の個人の公開鍵の登録をまとめて認証機関に依頼することが考えられる。例えば、企業内でその企業に勤務する者の公開鍵の登録を、その企業内の責任者がまとめて認証機関に依頼するような場合である。この場合、その企業に勤務する者が登録を申し出た公開鍵に対し、その企業内の責任者が、故意にその公開鍵に不正を加えたり偶発的に公開鍵に不正が加えられることが考えられる。

【０１７０】そこで、第７の実施の形態では、ある責任者が複数の登録申請者の公開鍵の登録をまとめて行なう場合に、その責任者の不正を防止するため、以下のような手順で登録を行なう。以下では、企業Ｄ内で公開鍵の登録を申請する申請者Ａの公開鍵を、登録責任者Ｂが、取りまとめて認証局（認証機関）Ｃに登録を依頼する場合を例に説明する。まず、登録の申請者Ａは、認証局Ｃの公開鍵で自分の公開鍵（登録を申請する公開鍵）を暗号化し、これを登録責任者Ｂに渡す。登録責任者Ｂは、申請者Ａから登録を申請された公開鍵に電子署名して、認証局Ｃに送付する。認証局Ｃでは、登録責任者Ｂによる電子署名により途中で改竄されていないことを確認した後、認証局Ｃの秘密鍵で登録申請者Ａの公開鍵を取り出し、登録申請者Ａの証明書を作成し、この証明書を企業Ｄの公開鍵で暗号化した後、企業Ｄの登録責任者Ｂあるいは登録申請者Ａに送付する。登録責任者Ｂに送付された場合は、当該証明書が登録申請者Ａに必ず渡されるという保障が無いため、認証局Ｃは、当該証明書を企業Ｄの公開鍵以外に登録申請者Ａの公開鍵で暗号化して送付するようにしても良い。

【０１７１】図４３は、第７の実施の形態における公開鍵登録の手順を示すフローチャートである。ステップ４３０１～４２０４は登録申請者Ａの処理フロー、ステップ４３０５，４３０６および４３１３，４３１４は登録責任者Ｂの処理フロー、ステップ４３０７～４３１２は認証局Ｃの処理フローを、それぞれ示す。

【０１７２】まず登録申請者Ａは、ステップ４３１０で公開鍵を生成し、ステップ４３０２で認証局Ｃの公開鍵を入手する。次にステップ４３０３で認証局Ｃの公開鍵で自分の公開鍵を暗号化し、ステップ４３０４で暗号化した自分の公開鍵を登録責任者Ｂに渡してその公開鍵の登録を申請する。図示しないが、他の登録申請者も同様にして暗号化した公開鍵を登録責任者Ｂに渡し登録を申請するが、処理は同様であるので以下では登録申請者Ａのみに着目して説明する。

【０１７３】登録責任者Ｂは、ステップ４３０５で、受付けた登録申請者Ａの暗号化公開鍵およびその他の必要な情報をまとめて証明書発行依頼書を作成し、自分の秘密鍵で電子署名を行ない、ステップ４３０６でその電子署名付き証明書発行依頼書を認証局Ｃに送付する。

【０１７４】認証局Ｃでは、ステップ４３０７で、登録

責任者Bから送付された電子署名付き証明書発行依頼書の署名を確認し、当該証明書発行依頼書が確かに登録責任者Bから送られたものであってかつ改竄されていないかどうか判別する。登録責任者Bからであってかつ改竄されていないときは、ステップ4309で、当該証明書発行依頼書に含まれている暗号化された登録申請者Aの公開鍵を認証局Cの秘密鍵で復号する。ステップ4310で、登録申請者Aの公開鍵の証明書を作成する。ステップ4311でその証明書を企業Dの公開鍵で暗号化し、ステップ4312で認証書を発行し、ステップ4313に進む。ステップ4307で証明書発行依頼書が登録責任者Bからのもので無い場合、または証明書発行依頼書が改竄されていたときは、ステップ4308で、登録責任者Bにその旨を通知し改竄されていた登録申請者の暗号化公開鍵を破棄する。なお、図43のフローチャートでは、ステップ4308で改竄されている暗号化公開鍵のみを破棄し、正当なものと思われる暗号化公開鍵については、ステップ4309以降の処理を行なうこととしている。ただし、一つでも登録申請者の公開鍵に改竄が加えられていると判別されたときは、ステップ4308の後、処理を終了してもよい。

【0175】登録責任者Bは、ステップ4313で、認証局Cから送付された認証書を受け取り、企業Dの秘密鍵で復号して登録申請者Aの公開鍵の証明書を得、ステップ4314でその証明書を登録申請者Aに配布する。

【0176】この第7の実施の形態によれば、企業D内において公開鍵の登録を登録責任者Bが取りまとめて行なう際に、偶発的あるいは故意に未登録の公開鍵に不正が加えられることを防ぎ、確かに登録責任者B（企業D）により依頼されたことを保証し、また認証局Cからの証明書を確実に企業Dに送付することが可能となる。企業D内において公開鍵の登録をまとめて行なう場合は、登録申請者の審査のためその上司・人事・総務などの各部門を経由して最終的に登録責任者Bが認証局Cに証明書の発行依頼をすることが考えられるが、この審査過程での偶発的あるいは故意に行なわれる不正も防ぐことができる。認証局Cが証明書を送付する際に、企業Dの公開鍵以外に登録申請者Aの公開鍵で暗号化して送付するようにすれば、証明書を安全・確実に登録申請者Aに渡せる。

【0177】

【発明の効果】以上説明したように、本発明によれば、オープンなネットワーク環境において電子商取引を行なう際に必要とされる認証・公証サービス（電子情報署名・保管サービス）が実際に実現できる。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態に係る電子公証システムのシステム図である。

【図2】本発明の第1の実施の形態におけるICカードの内部構成図である。

【図3】本発明の第1の実施の形態におけるサービス提供装置の内部構成図である。

【図4】本発明の第1の実施の形態におけるサービス享受装置の内部構成図である。

【図5】本発明の第1の実施の形態におけるICカード内のデータ記憶領域の中身を示すブロック図である。

【図6】本発明の第1の実施の形態において、サービス提供者が認証機関よりICカードを発行してもらう手順を示す流れ図である。

【図7】本発明の第1の実施の形態において、サービス提供者が、自ICカードとサービス提供装置とを用いて認証機関より証明書を発行してもらう手順を示す流れ図である。

【図8】本発明の第1の実施の形態の変形例であり、サービス提供者が認証機関より証明書格納済みのICカードを発行してもらう手順を示す流れ図である。

【図9】本発明の第1の実施の形態において、サービス提供者およびサービス享受者の間で行われるサービス処理の全体手順を示す流れ図である。

【図10】本発明の第1の実施の形態における一者署名付き契約情報の一例である。

【図11】本発明の第1の実施の形態における一者署名付き契約情報のもう一つの例である。

【図12】本発明の第1の実施の形態における三者署名付き契約情報の一例である。

【図13】本発明の第1の実施の形態において、サービス享受装置とICカードとが連動して一者署名付き契約情報を生成する手順の詳細を示す流れ図である。

【図14】本発明の第1の実施の形態において、サービス提供装置とICカードとが連動して三者署名付き契約情報を生成する手順の詳細を示す流れ図である。

【図15】本発明の第2の実施の形態に係る電子公証システムのシステム図である。

【図16】本発明の第2の実施の形態におけるICカードの内部構成図である。

【図17】本発明の第2の実施の形態において、サービス享受装置とICカードとが連動して一者署名付き契約情報を生成する手順の詳細を示す流れ図である。

【図18】本発明の第2の実施の形態において、サービス提供装置とICカードとが連動して三者署名付き契約情報を生成する手順の詳細を示す流れ図である。

【図19】本発明の第2の実施の形態において、サービス提供装置が時刻管理機関から標準時刻を取得する手順を示す流れ図である。

【図20】本発明の第3の実施の形態に係る電子公証システムのシステム図である。

【図21】本発明の第3の実施の形態におけるICカードの内部構成図である。

【図22】本発明の第3の実施の形態において、サービス享受装置とICカードと時刻管理機関とが連動して一

者署名付き契約情報を生成する手順の詳細を示す流れ図である。

【図２３】本発明の第３の実施の形態において、サービス提供装置とＩＣカードと時刻管理機関とが連動して三者署名付き契約情報を生成する手順の詳細を示す流れ図である。

【図２４】本発明の第４の実施の形態に係る電子公証システムのシステム図である。

【図２５】本発明の第４の実施の形態におけるサービス提供装置の内部構成図である。

【図２６】本発明の第４の実施の形態におけるサービス享受装置の内部構成図である。

【図２７】本発明の第４の実施の形態におけるフロッピーディスクの中身を示すブロック図である。

【図２８】本発明の第４の実施の形態において、サービス提供者が認証機関よりフロッピーディスクを発行してもらう手順を示す流れ図である。

【図２９】本発明の第４の実施の形態において、サービス提供者が、自フロッピーディスクとサービス提供装置とを用いて認証機関より証明書を発行してもらう手順を示す流れ図である。

【図３０】本発明の第４の実施の形態において、サービス享受装置が一者署名付き契約情報を生成する手順の詳細を示す流れ図である。

【図３１】本発明の第４の実施の形態において、サービス提供装置が三者署名付き契約情報を生成する手順の詳細を示す流れ図である。

【図３２】本発明の第５の実施の形態におけるＩＣカードの内部構成図である。

【図３３】本発明の第６の実施の形態のシステム構成図である。

【図３４】本発明の第６の実施の形態における会員証データベースの内部構造図である。

＊【図３５】本発明の第６の実施の形態における会員登録の手順を示す流れ図である。

【図３６】本発明の第６の実施の形態における会員登録抹消の手順を示す流れ図である。

【図３７】本発明の第６の実施の形態における会員間で何らかの取引を行なうとき相手を確認するための手順を示す流れ図である。

【図３８】本発明の第６の実施の形態における会員認証局の端末の制御モジュールの処理手順を示す流れ図である。

【図３９】本発明の第６の実施の形態における会員認証局の端末の会員登録モジュールの処理手順（その１）を示す流れ図である。

【図４０】本発明の第６の実施の形態における会員認証局の端末の会員登録モジュールの処理手順（その２）を示す流れ図である。

【図４１】本発明の第６の実施の形態における会員認証局の端末の会員登録抹消モジュールの処理手順を示す流れ図である。

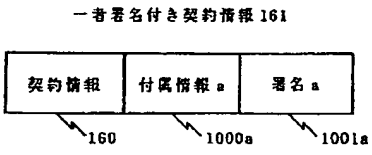
【図４２】本発明の第６の実施の形態における会員認証局の端末の会員認証モジュールの処理手順を示す流れ図である。

【図４３】本発明の第７の実施の形態における公開鍵登録の手順を示す流れ図である。

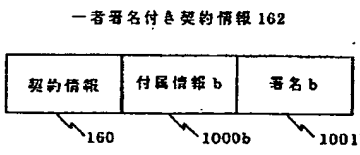
【符号の説明】

１００…サービス提供者、１１０，１１１…サービス享受者、１２０，１２１，１２２，１２３…ＩＣカード、１３０…サービス提供装置、１４０，１４１…サービス享受装置、１５０，１５１，１５２…公開鍵、１５３，１５４，１５５…証明書、１６０…契約情報、１６１，１６２…一者署名付き契約情報、１６３…三者署名付き契約情報、１７０…認証機関、１８０…通信網。

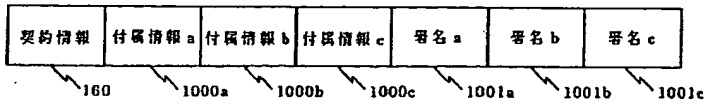
【図１０】



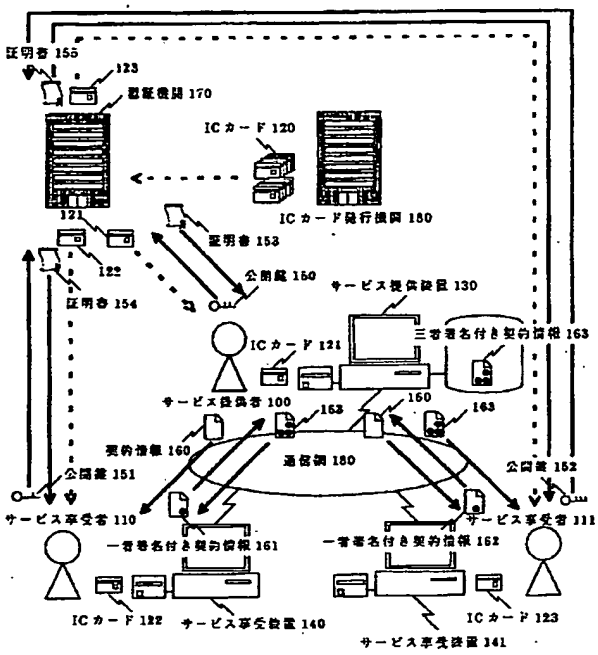

【図１１】



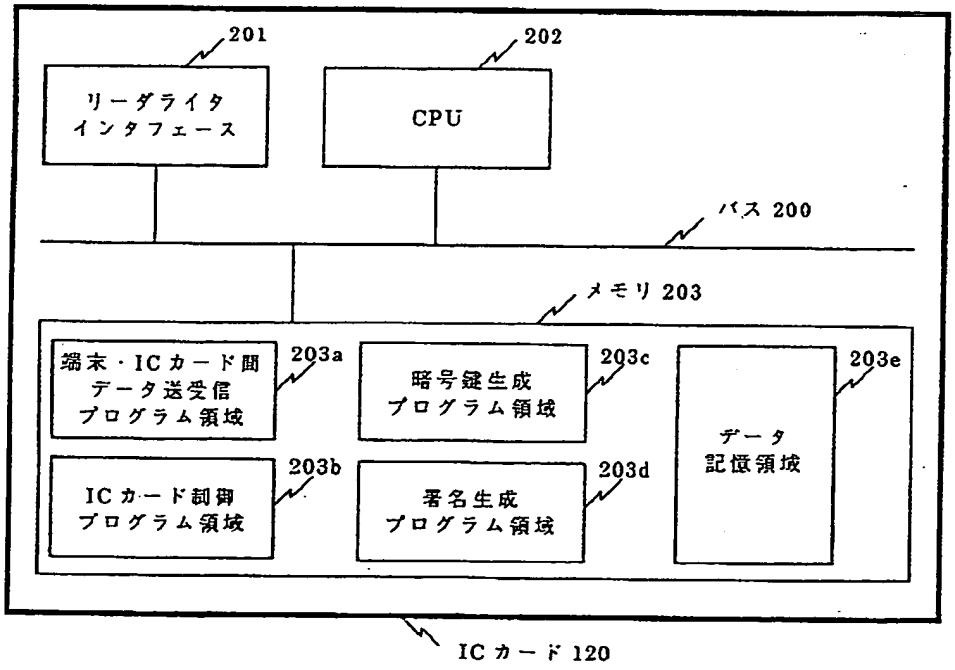

【図１２】



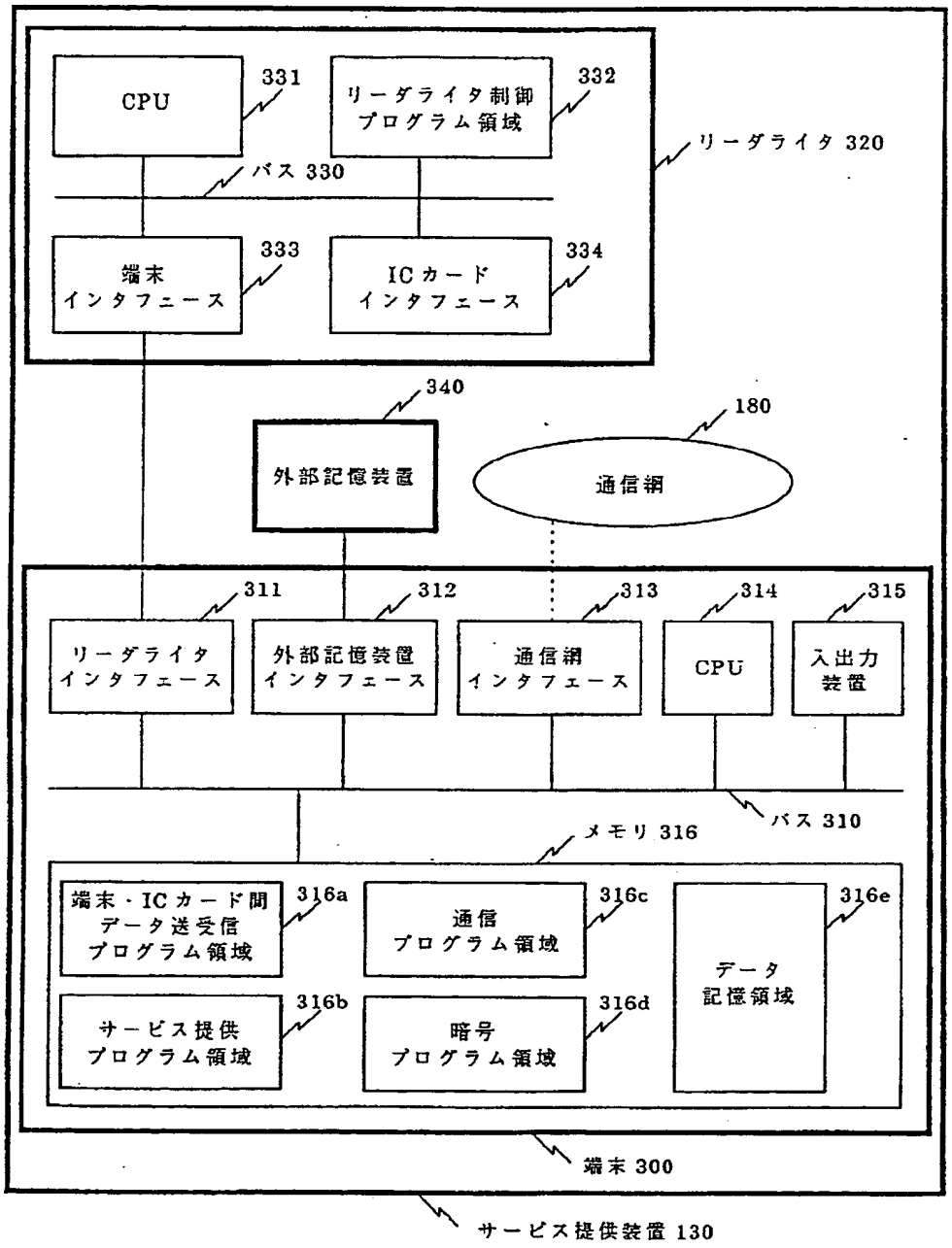
【図1】


証明書 155
123
認証機関 170
ICカード 120
121
ICカード発行機関 180
証明書 153
122
公開鍵 150
証明書 154
サービス提供装置 130
ICカード 121
三者署名付き契約情報 163
サービス提供者 100
160
162
163
契約情報 160
通信網 180
公開鍵 151
公開鍵 152
サービス享受者 110
サービス享受者 111
一者署名付き契約情報 161
一者署名付き契約情報 162
ICカード 122
サービス享受装置 140
ICカード 123
サービス享受装置 141

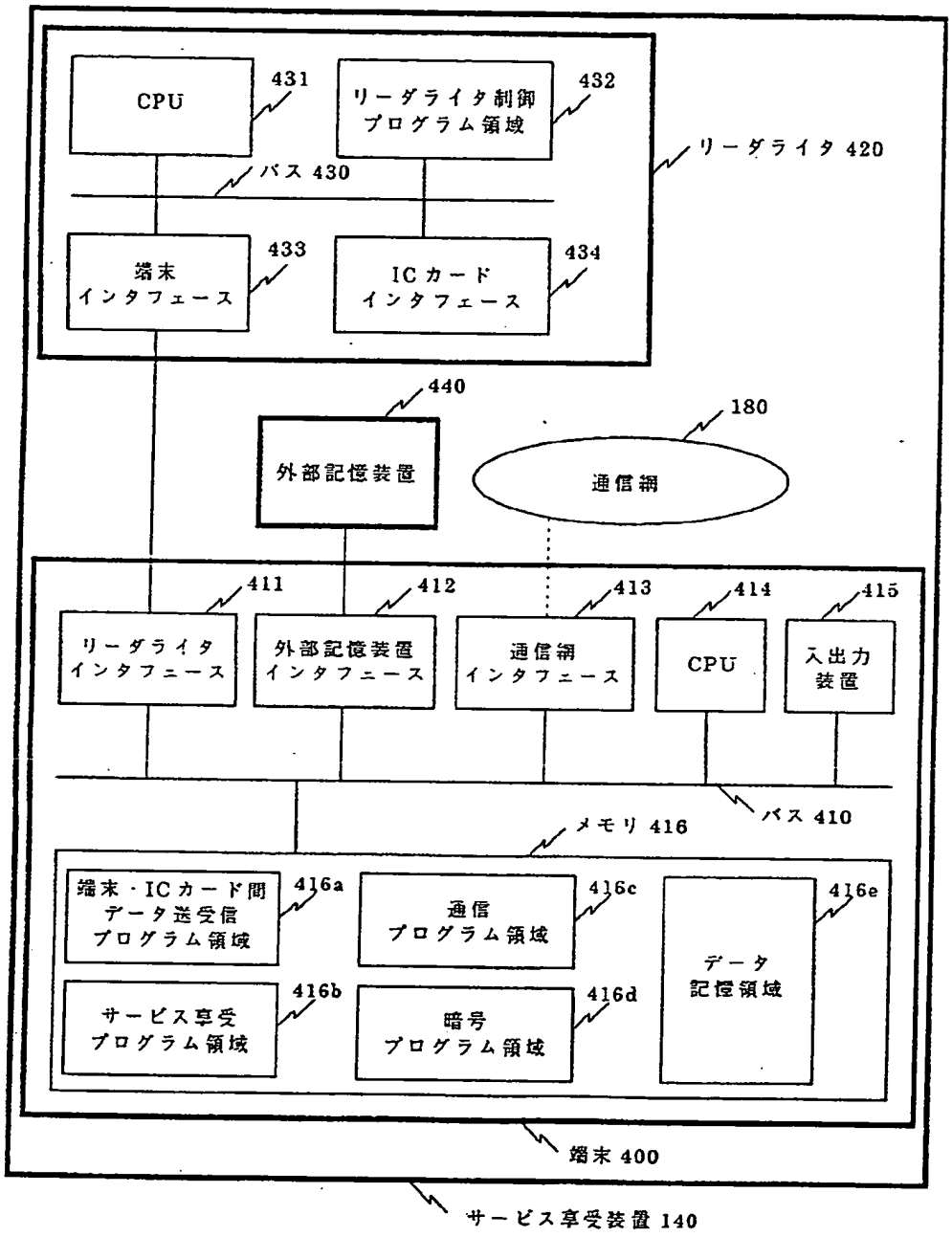
【図2】


201
202
リーダライタ
インタフェース
CPU
バス 200
メモリ 203
端末・ICカード間
データ送受信
プログラム領域
203a
暗号鍵生成
プログラム領域
203c
データ
記憶領域
203e
ICカード制御
プログラム領域
203b
署名生成
プログラム領域
203d
ICカード 120

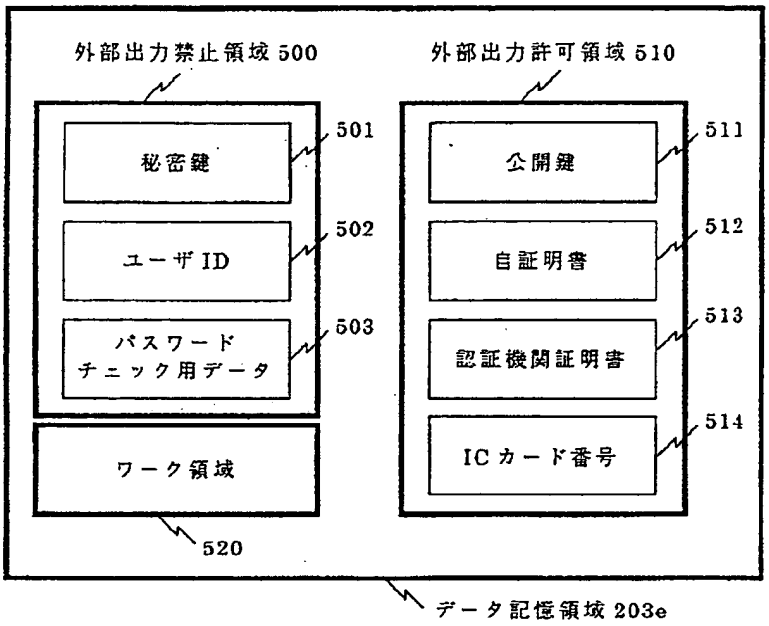
【図3】


CPU
331
リーダライタ制御プログラム領域
332
リーダライタ 320
バス 330
端末インタフェース
333
ICカードインタフェース
334
340
外部記憶装置
180
通信網
311
312
313
314
315
リーダライタインタフェース
外部記憶装置インタフェース
通信網インタフェース
CPU
入出力装置
バス 310
メモリ 316
端末・ICカード間データ送受信プログラム領域
316a
通信プログラム領域
316c
データ記憶領域
316e
サービス提供プログラム領域
316b
暗号プログラム領域
316d
端末 300
サービス提供装置 130

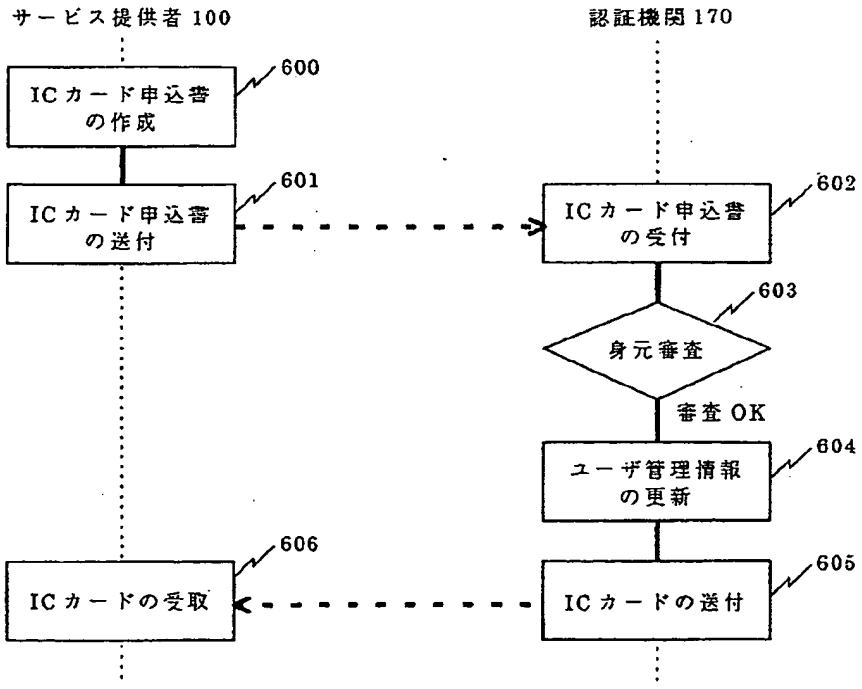
【図4】


CPU
431
リーダライタ制御プログラム領域
432
リーダライタ 420
バス 430
端末インタフェース
433
ICカードインタフェース
434
440
外部記憶装置
180
通信網
411
412
413
414
415
リーダライタインタフェース
外部記憶装置インタフェース
通信網インタフェース
CPU
入出力装置
バス 410
メモリ 416
端末・ICカード間データ送受信プログラム領域
416a
通信プログラム領域
416c
データ記憶領域
416e
サービス享受プログラム領域
416b
暗号プログラム領域
416d
端末 400
サービス享受装置 140

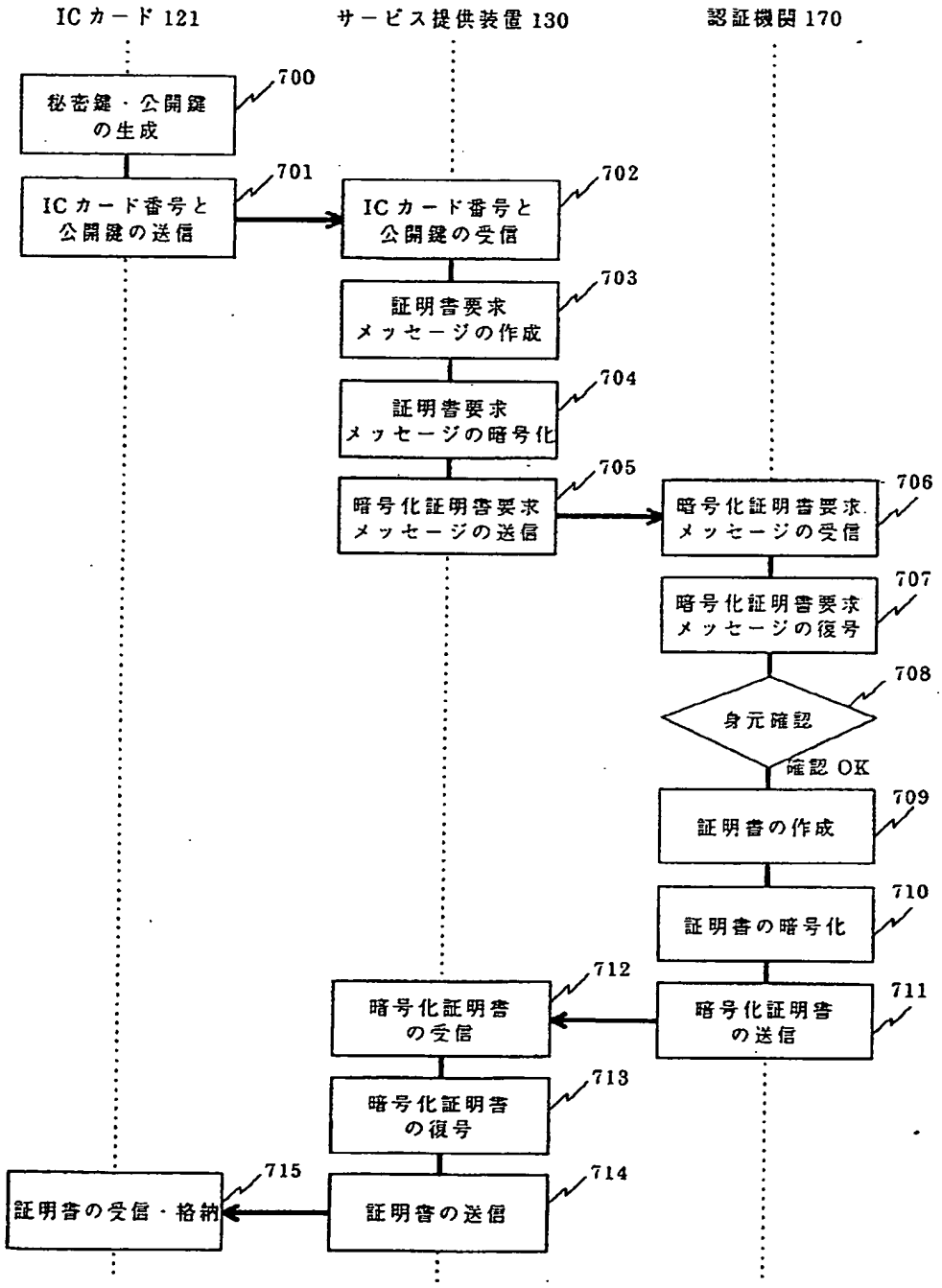
【図5】


外部出力禁止領域 500
外部出力許可領域 510
秘密鍵
501
ユーザ ID
502
パスワード
チェック用データ
503
ワーク領域
520
公開鍵
511
自証明書
512
認証機関証明書
513
IC カード番号
514
データ記憶領域 203e

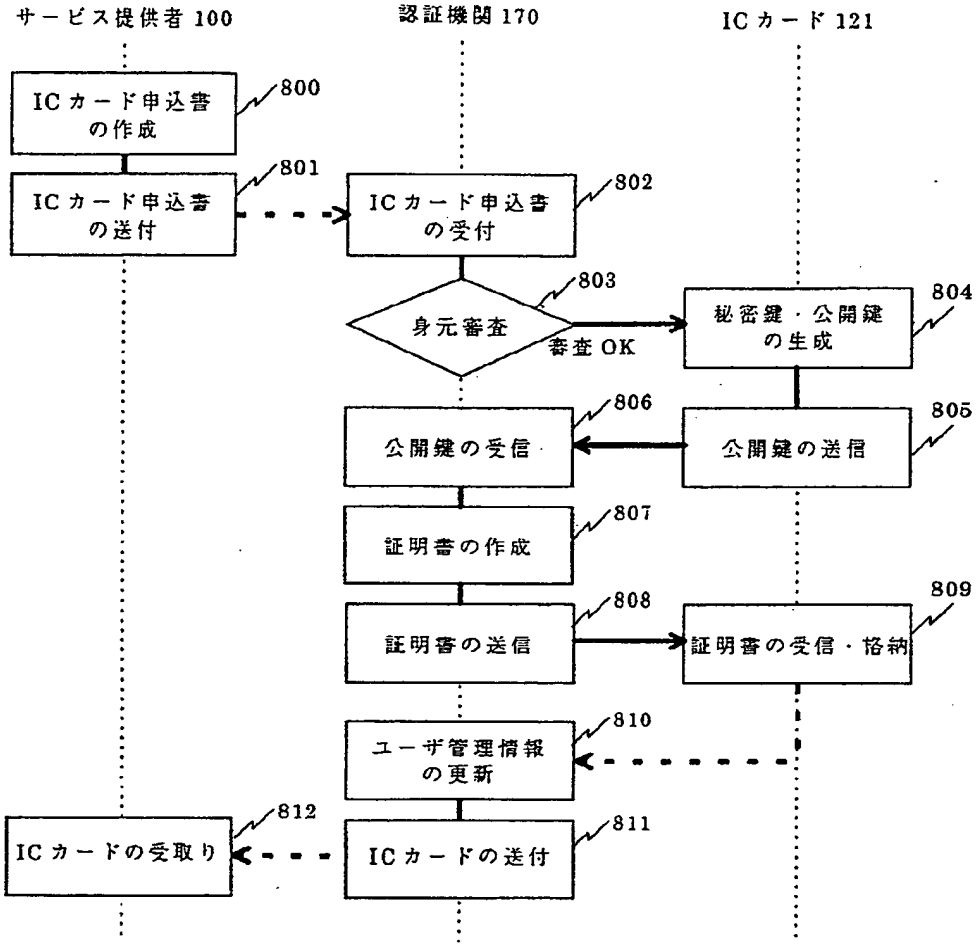
【図6】


サービス提供者 100
認証機関 170
IC カード申込書
の作成
600
IC カード申込書
の送付
601
IC カード申込書
の受付
602
身元審査
603
審査 OK
ユーザ管理情報
の更新
604
IC カードの送付
605
IC カードの受取
606

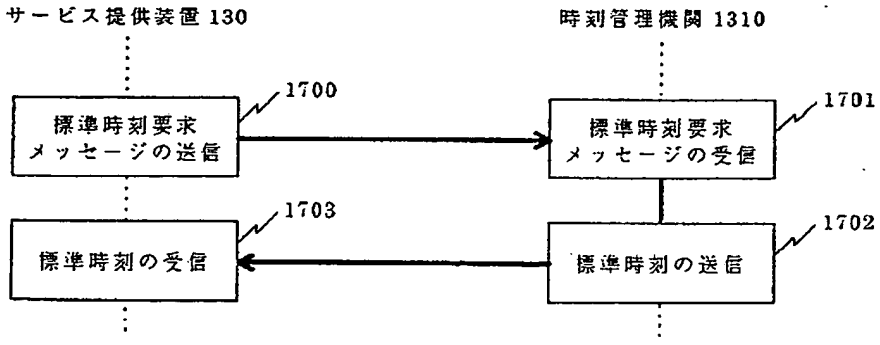
【図7】


ICカード 121
サービス提供装置 130
認証機関 170
秘密鍵・公開鍵の生成
700
ICカード番号と公開鍵の送信
701
ICカード番号と公開鍵の受信
702
証明書要求メッセージの作成
703
証明書要求メッセージの暗号化
704
暗号化証明書要求メッセージの送信
705
暗号化証明書要求メッセージの受信
706
暗号化証明書要求メッセージの復号
707
身元確認
708
確認 OK
証明書の作成
709
証明書の暗号化
710
暗号化証明書の送信
711
暗号化証明書の受信
712
暗号化証明書の復号
713
証明書の送信
714
証明書の受信・格納
715

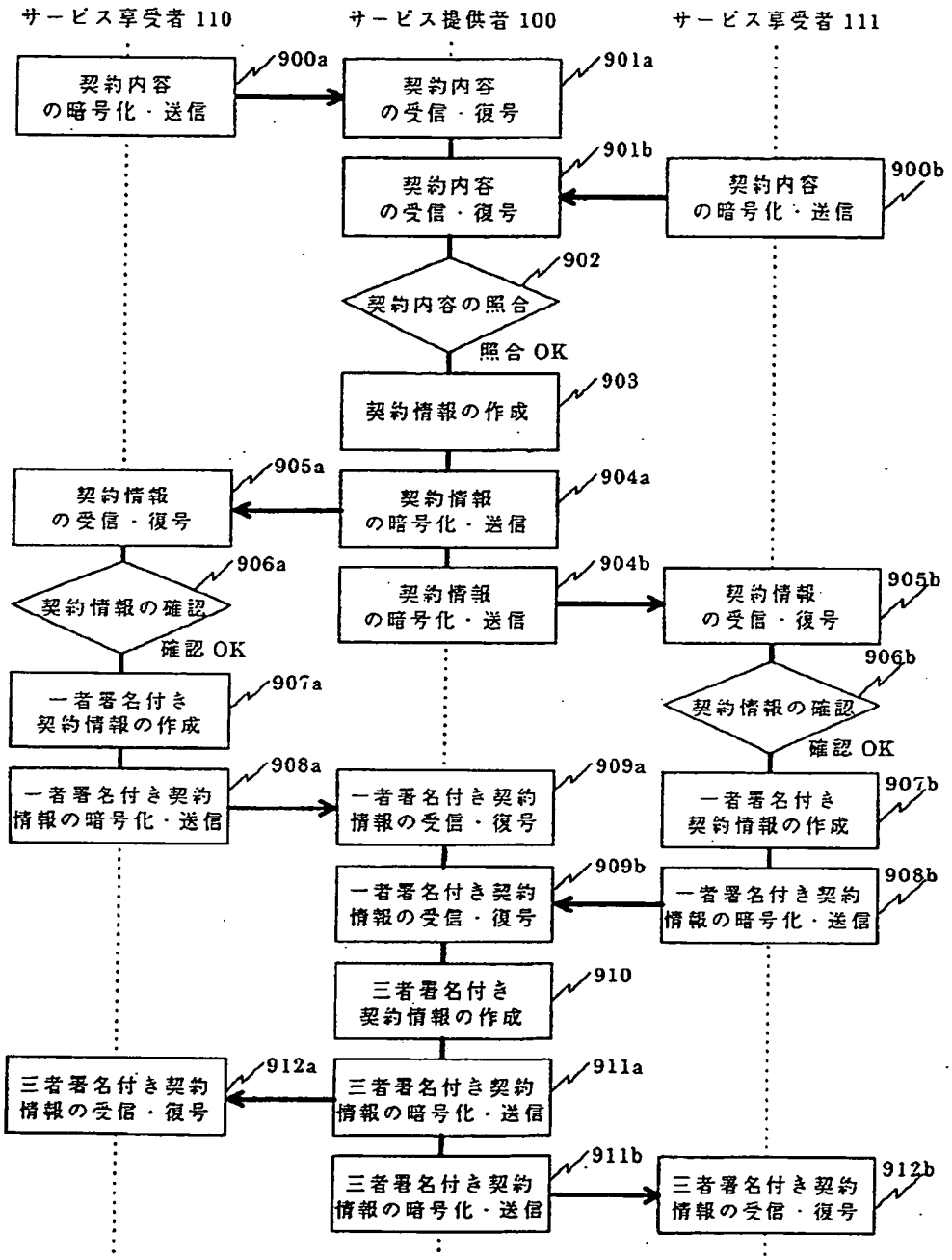
【図8】


サービス提供者 100
認証機関 170
ICカード 121
ICカード申込書の作成
800
ICカード申込書の送付
801
ICカード申込書の受付
802
身元審査
803
審査 OK
秘密鍵・公開鍵の生成
804
公開鍵の受信
806
公開鍵の送信
805
証明書の作成
807
証明書の送信
808
証明書の受信・格納
809
ユーザ管理情報の更新
810
ICカードの受取り
812
ICカードの送付
811

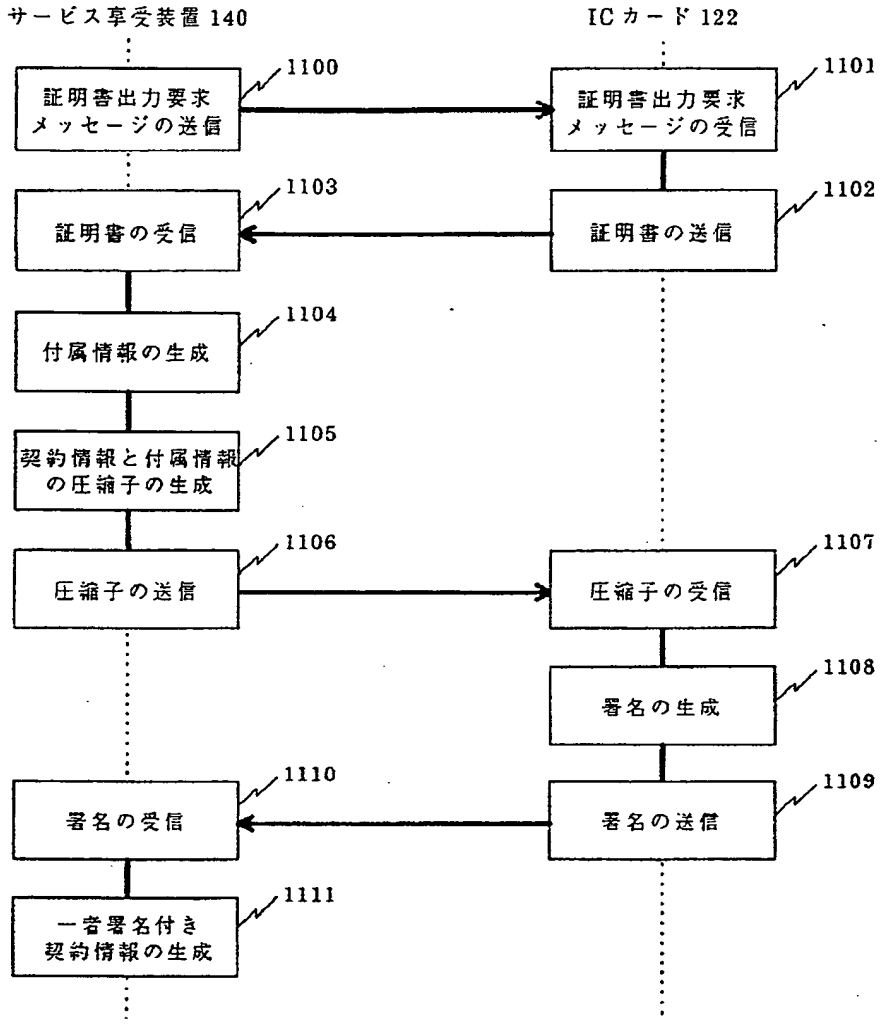
【図19】


サービス提供装置 130
時刻管理機関 1310
標準時刻要求メッセージの送信
1700
標準時刻要求メッセージの受信
1701
標準時刻の受信
1703
標準時刻の送信
1702

【図9】


サービス享受者 110
サービス提供者 100
サービス享受者 111
契約内容の暗号化・送信
900a
契約内容の受信・復号
901a
契約内容の受信・復号
901b
契約内容の暗号化・送信
900b
契約内容の照合
902
照合 OK
契約情報の作成
903
契約情報の受信・復号
905a
契約情報の暗号化・送信
904a
契約情報の確認
906a
確認 OK
契約情報の暗号化・送信
904b
契約情報の受信・復号
905b
一者署名付き契約情報の作成
907a
契約情報の確認
906b
確認 OK
一者署名付き契約情報の暗号化・送信
908a
一者署名付き契約情報の受信・復号
909a
一者署名付き契約情報の作成
907b
一者署名付き契約情報の受信・復号
909b
一者署名付き契約情報の暗号化・送信
908b
三者署名付き契約情報の作成
910
三者署名付き契約情報の受信・復号
912a
三者署名付き契約情報の暗号化・送信
911a
三者署名付き契約情報の暗号化・送信
911b
三者署名付き契約情報の受信・復号
912b

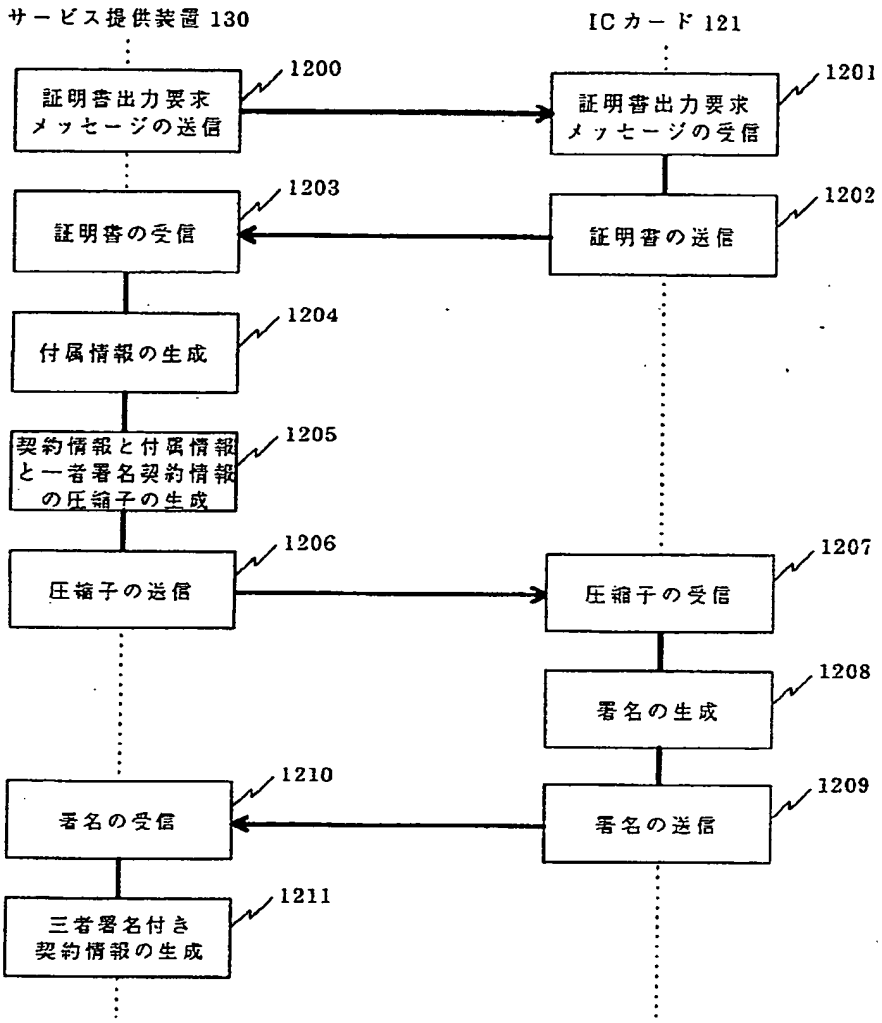
【図13】



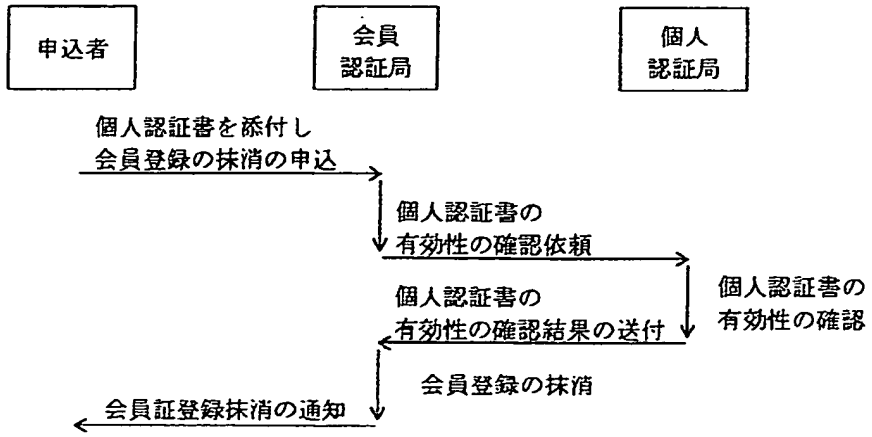

【図34】

| 会員証番号 | 会員名 | 個人認証書番号 | 有効期間 | | 会員の公開鍵 | | 予備 |
|---|---|---|---|---|---|---|---|
| | | | 開始日時 | 終了日時 | 鍵のｱﾙｺﾞﾘｽﾞﾑ | 鍵(ﾋﾞｯﾄ列) | |
| | | | | | | | |

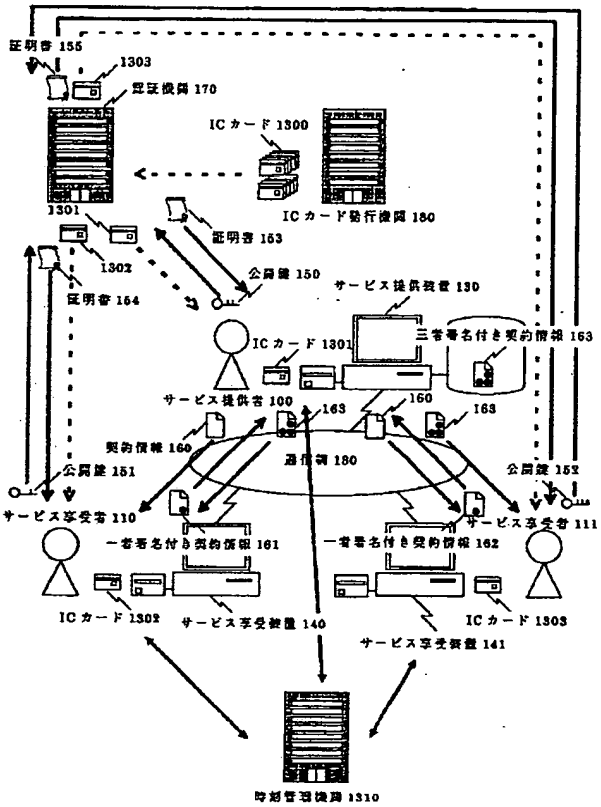
【図14】


サービス提供装置 130
ICカード 121
証明書出力要求メッセージの送信
1200
証明書出力要求メッセージの受信
1201
証明書の受信
1203
証明書の送信
1202
付属情報の生成
1204
契約情報と付属情報と一者署名契約情報の圧縮子の生成
1205
圧縮子の送信
1206
圧縮子の受信
1207
署名の生成
1208
署名の受信
1210
署名の送信
1209
三者署名付き契約情報の生成
1211

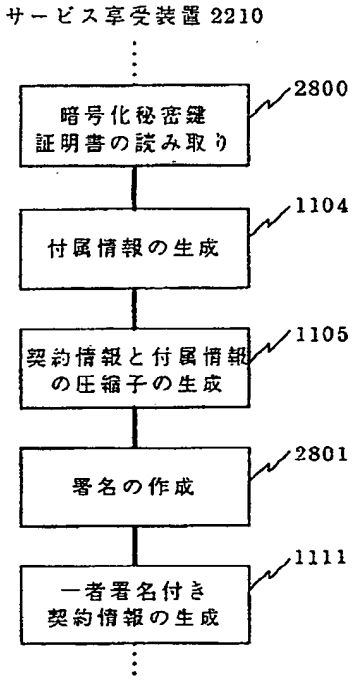
【図36】


申込者
会員認証局
個人認証局
個人認証書を添付し会員登録の抹消の申込
個人認証書の有効性の確認依頼
個人認証書の有効性の確認結果の送付
個人認証書の有効性の確認
会員登録の抹消
会員証登録抹消の通知

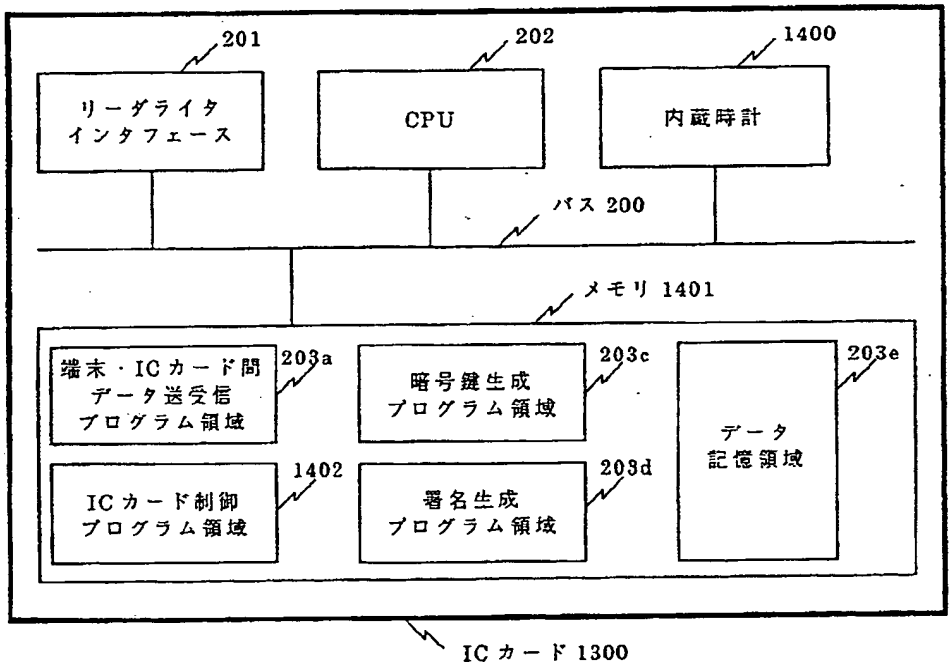
【図15】


証明書 155
1303
ICカード 1300
1301
ICカード発行機関 180
証明書 153
1302
公開鍵 150
証明書 164
サービス提供装置 130
ICカード 1301
三者署名付き契約情報 163
サービス提供者 100
163
160
163
契約情報 160
通信網 180
公開鍵 151
公開鍵 152
サービス享受者 110
サービス享受者 111
一者署名付き契約情報 161
一者署名付き契約情報 162
ICカード 1302
サービス享受装置 140
サービス享受装置 141
ICカード 1303
時刻管理機関 1310

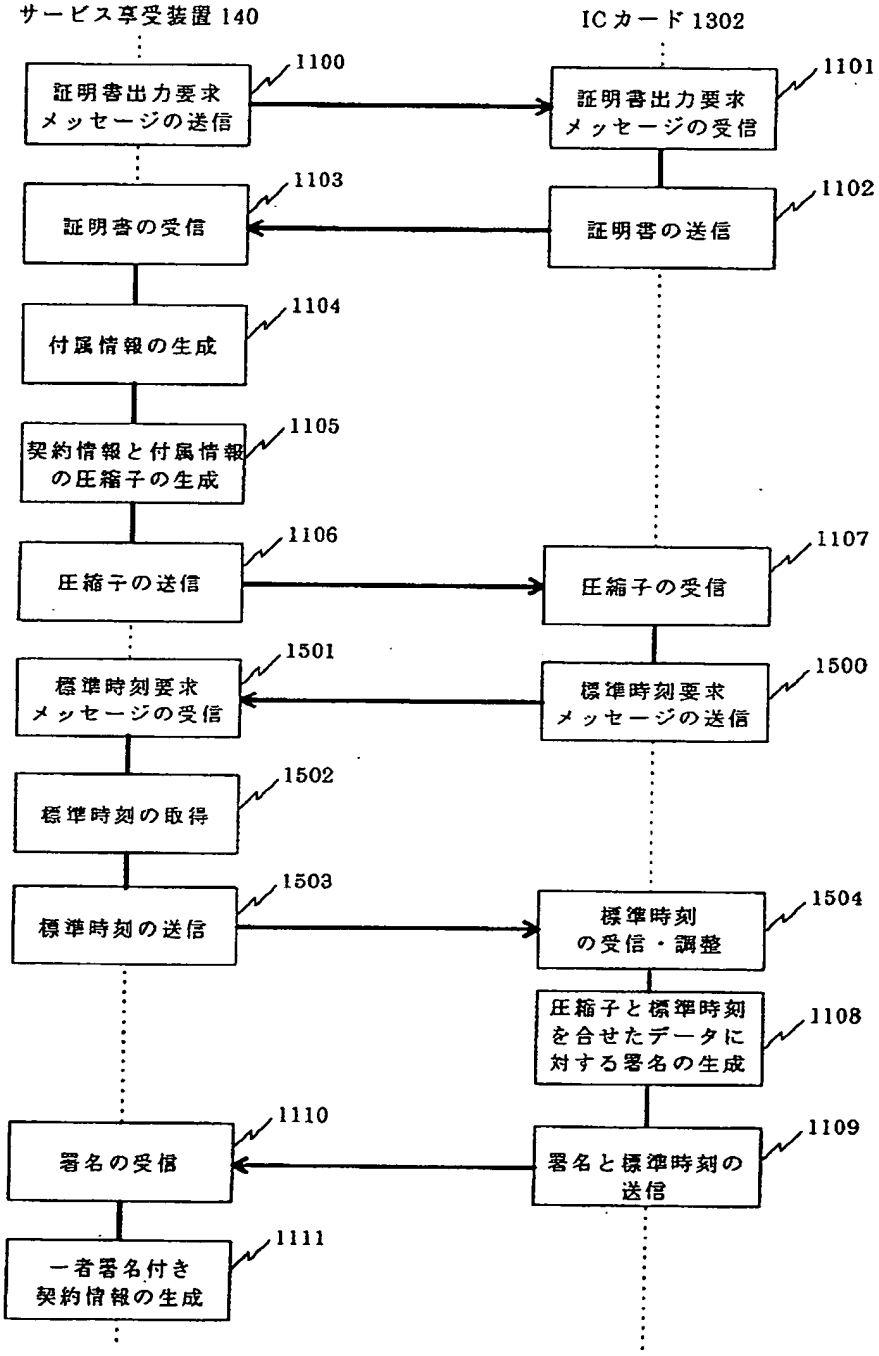
【図30】


サービス享受装置 2210
暗号化秘密鍵
証明書の読み取り
2800
付属情報の生成
1104
契約情報と付属情報
の圧縮子の生成
1105
署名の作成
2801
一者署名付き
契約情報の生成
1111

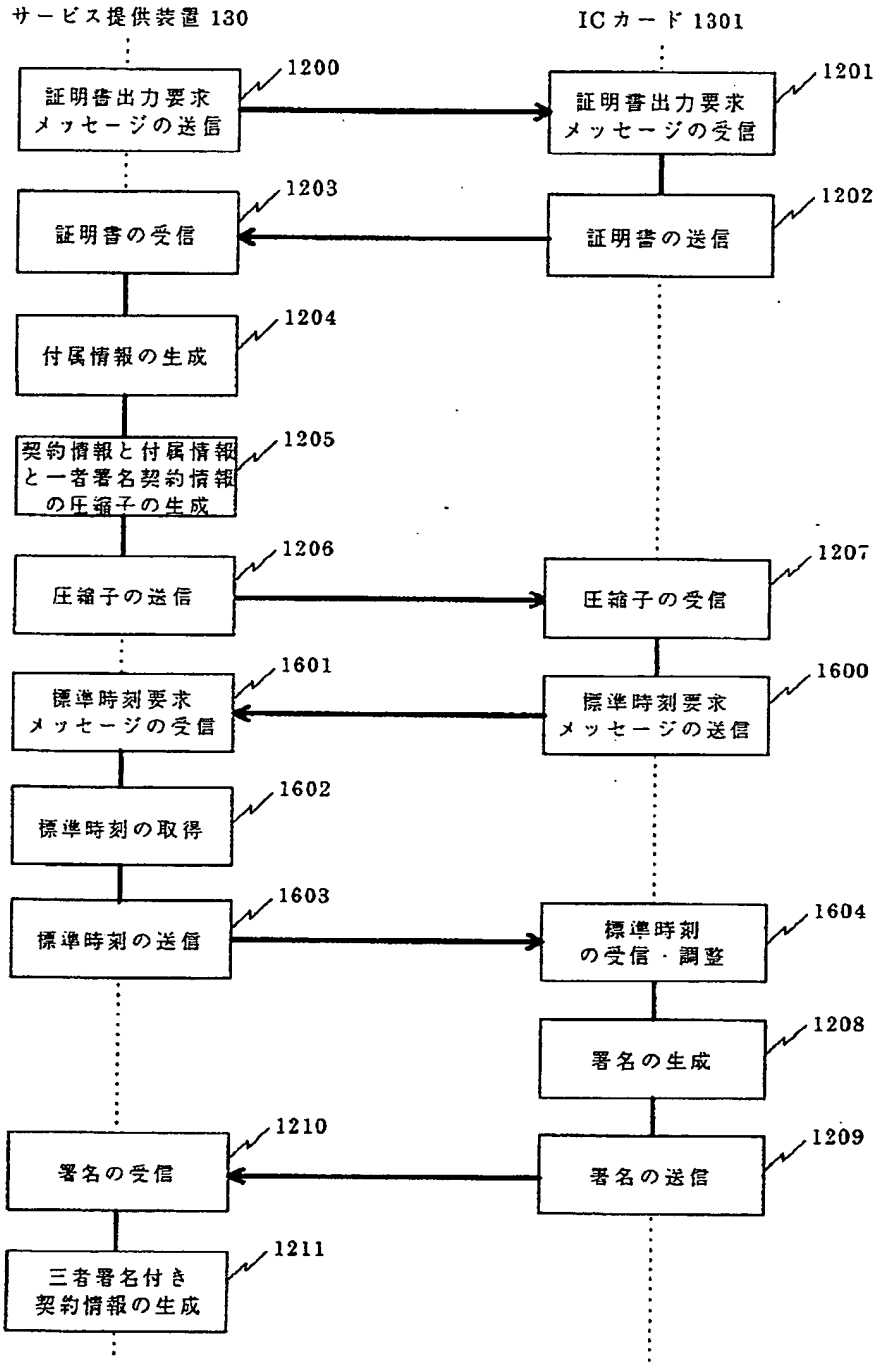
【図16】


201
リーダライタ
インタフェース
202
CPU
1400
内蔵時計
バス 200
メモリ 1401
端末・ICカード間
データ送受信
プログラム領域
203a
暗号鍵生成
プログラム領域
203c
データ
記憶領域
203e
ICカード制御
プログラム領域
1402
署名生成
プログラム領域
203d
ICカード 1300

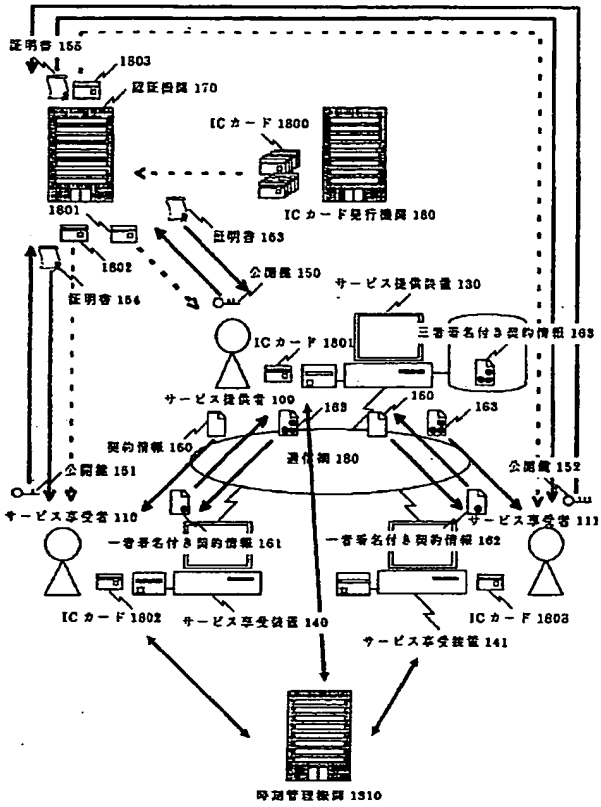
【図17】


サービス享受装置 140
ICカード 1302
証明書出力要求メッセージの送信
1100
証明書出力要求メッセージの受信
1101
証明書の受信
1103
証明書の送信
1102
付属情報の生成
1104
契約情報と付属情報の圧縮子の生成
1105
圧縮子の送信
1106
圧縮子の受信
1107
標準時刻要求メッセージの受信
1501
標準時刻要求メッセージの送信
1500
標準時刻の取得
1502
標準時刻の送信
1503
標準時刻の受信・調整
1504
圧縮子と標準時刻を合せたデータに対する署名の生成
1108
署名の受信
1110
署名と標準時刻の送信
1109
一者署名付き契約情報の生成
1111

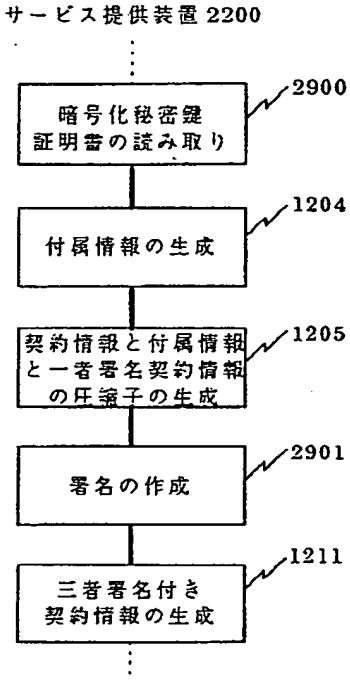
【図18】


サービス提供装置 130
ICカード 1301
証明書出力要求メッセージの送信
1200
証明書出力要求メッセージの受信
1201
証明書の受信
1203
証明書の送信
1202
付属情報の生成
1204
契約情報と付属情報と一者署名契約情報の圧縮子の生成
1205
圧縮子の送信
1206
圧縮子の受信
1207
標準時刻要求メッセージの受信
1601
標準時刻要求メッセージの送信
1600
標準時刻の取得
1602
標準時刻の送信
1603
標準時刻の受信・調整
1604
署名の生成
1208
署名の受信
1210
署名の送信
1209
三者署名付き契約情報の生成
1211

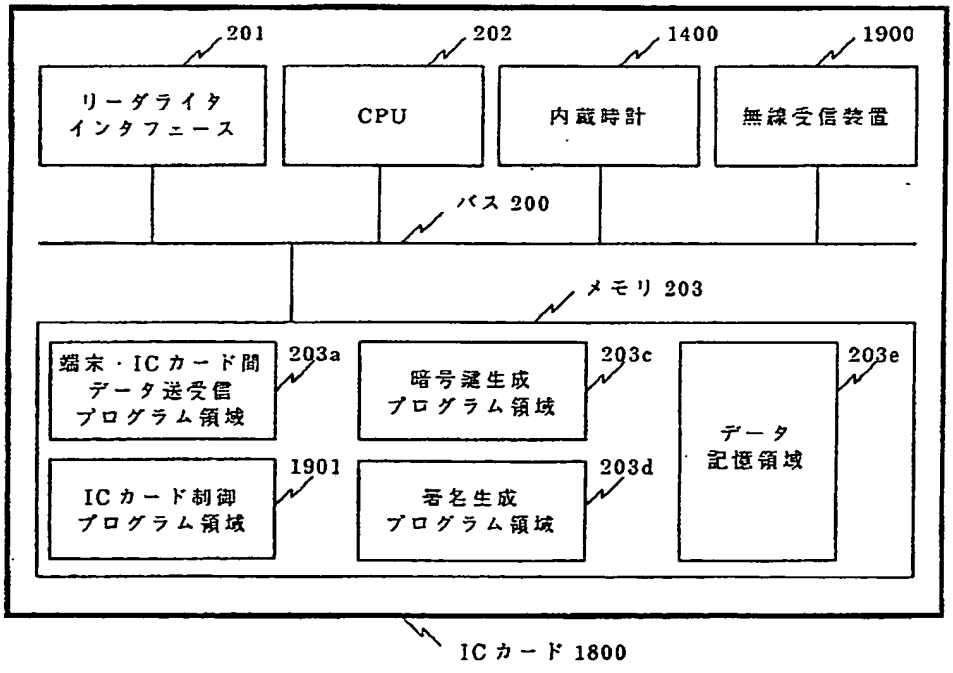
【図20】


証明書 155
1803
認証局 170
ICカード 1800
1801
ICカード発行機関 180
証明書 163
1802
公開鍵 150
証明書 154
サービス提供装置 130
ICカード 1801
三者署名付き契約情報 163
サービス提供者 100
160
163
契約情報 160
通信網 180
公開鍵 151
公開鍵 152
サービス享受者 110
サービス享受者 111
一者署名付き契約情報 161
一者署名付き契約情報 162
ICカード 1802
サービス享受装置 140
サービス享受装置 141
ICカード 1803
時刻管理機関 1310

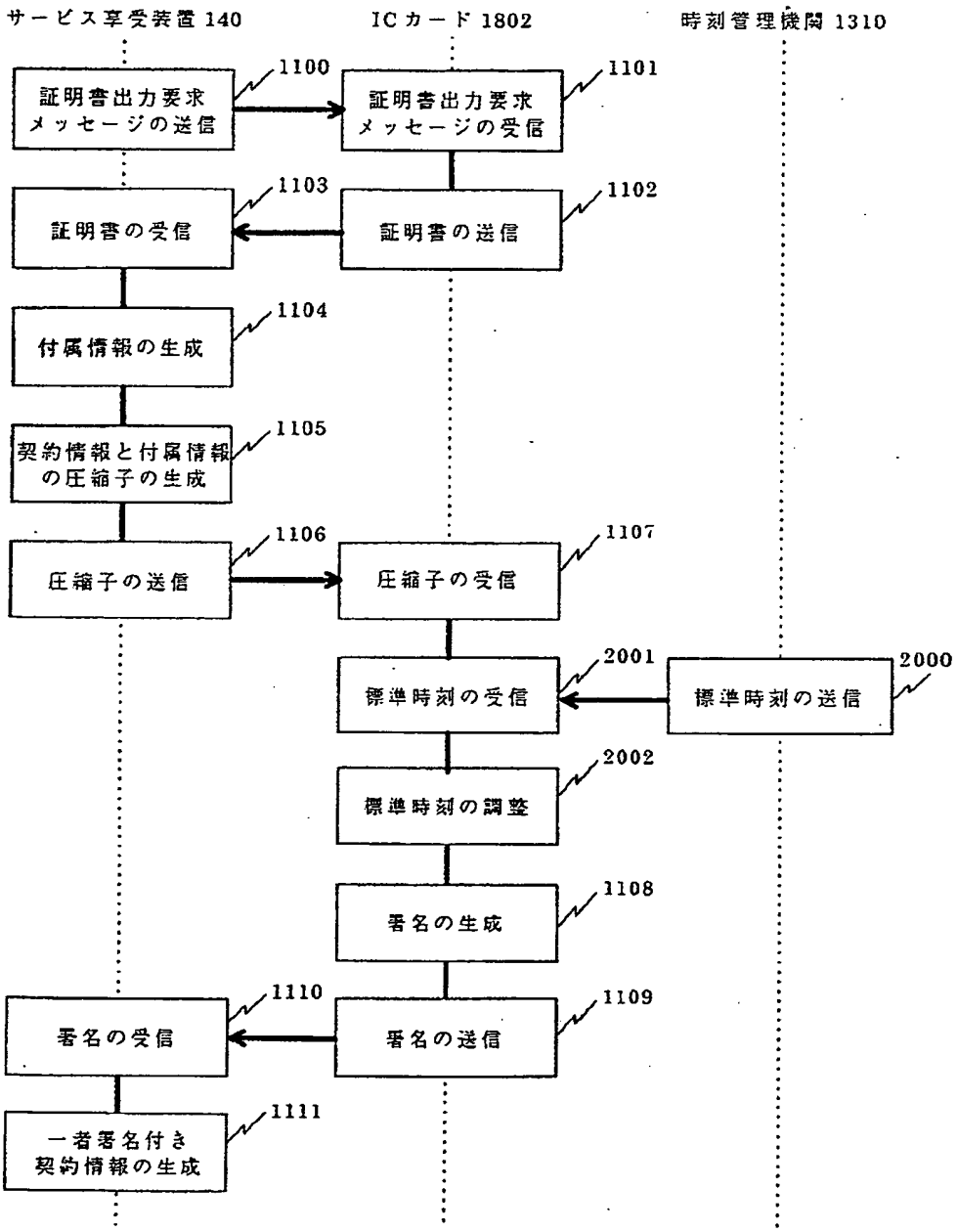
【図31】


サービス提供装置 2200
暗号化秘密鍵
証明書の読み取り
2900
付属情報の生成
1204
契約情報と付属情報
と一者署名契約情報
の圧縮子の生成
1205
署名の作成
2901
三者署名付き
契約情報の生成
1211

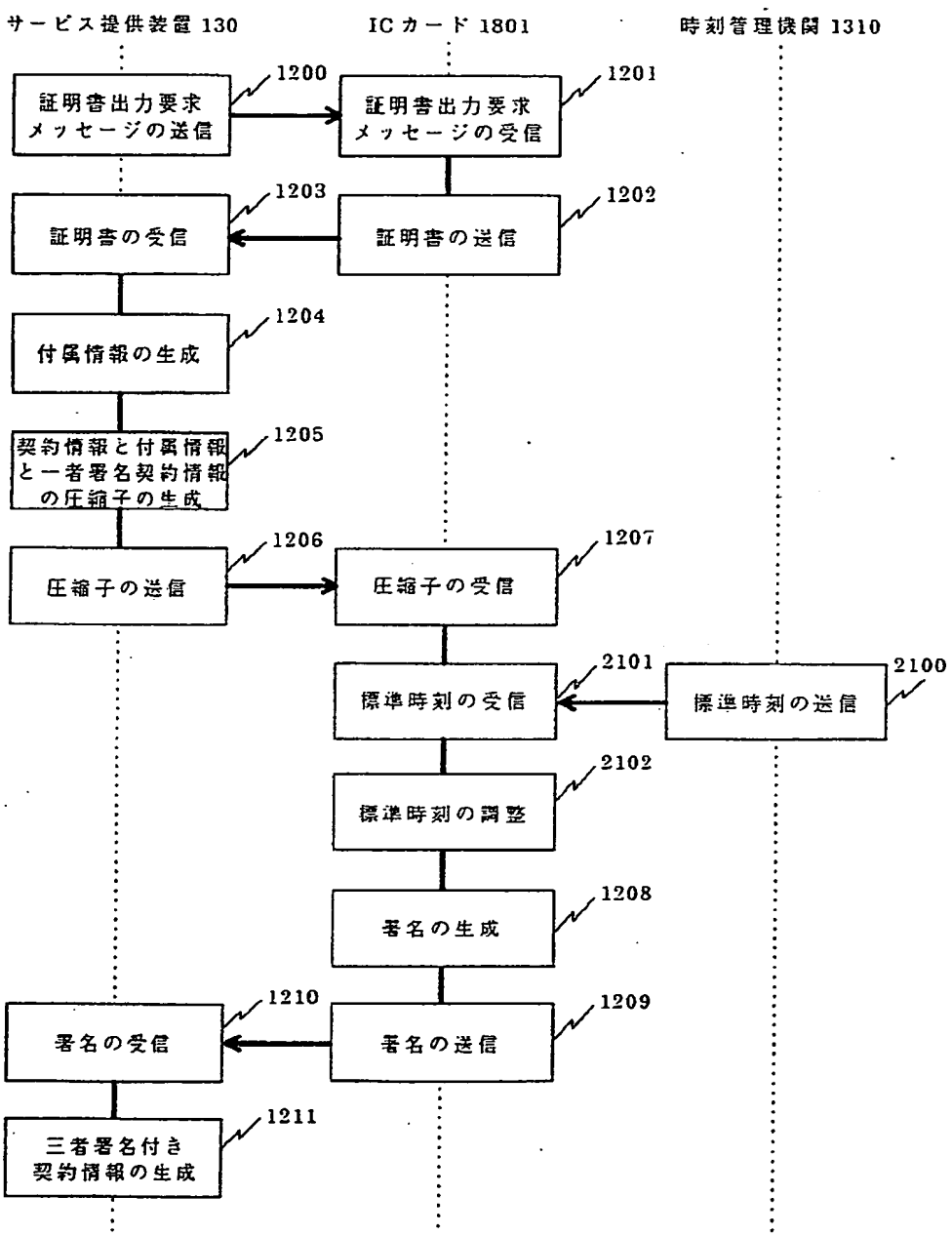
【図21】


201
リーダライタ
インタフェース
202
CPU
1400
内蔵時計
1900
無線受信装置
バス 200
メモリ 203
端末・ICカード間
データ送受信
プログラム領域
203a
暗号鍵生成
プログラム領域
203c
データ
記憶領域
203e
ICカード制御
プログラム領域
1901
署名生成
プログラム領域
203d
ICカード 1800

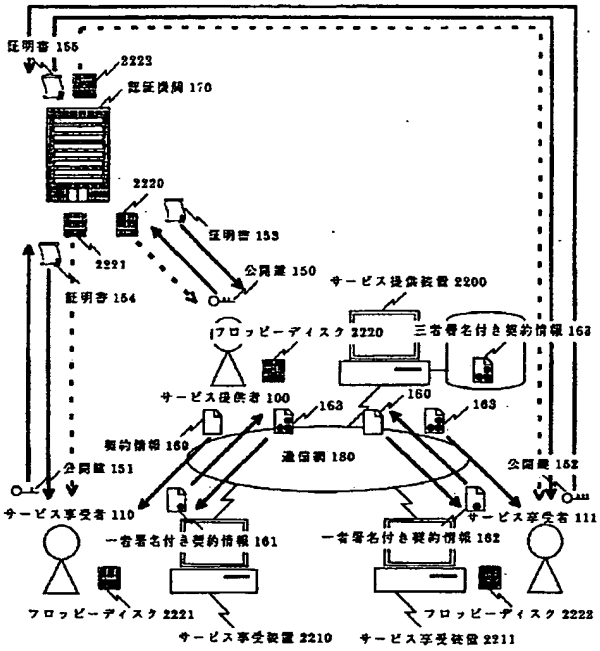
【図22】


サービス享受装置 140
ICカード 1802
時刻管理機関 1310
証明書出力要求メッセージの送信
1100
証明書出力要求メッセージの受信
1101
証明書の受信
1103
証明書の送信
1102
付属情報の生成
1104
契約情報と付属情報の圧縮子の生成
1105
圧縮子の送信
1106
圧縮子の受信
1107
標準時刻の受信
2001
標準時刻の送信
2000
標準時刻の調整
2002
署名の生成
1108
署名の受信
1110
署名の送信
1109
一者署名付き契約情報の生成
1111

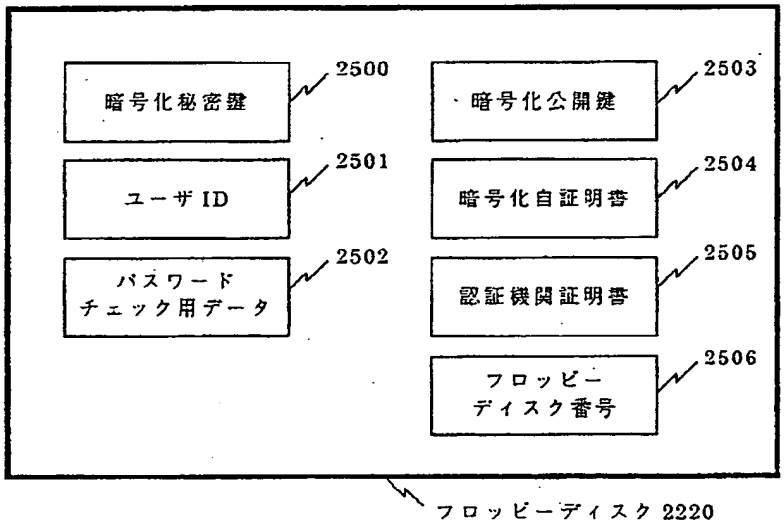
【図23】


サービス提供装置 130
ICカード 1801
時刻管理機関 1310
証明書出力要求メッセージの送信
1200
証明書出力要求メッセージの受信
1201
証明書の受信
1203
証明書の送信
1202
付属情報の生成
1204
契約情報と付属情報と一者署名契約情報の圧縮子の生成
1205
圧縮子の送信
1206
圧縮子の受信
1207
標準時刻の受信
2101
標準時刻の送信
2100
標準時刻の調整
2102
署名の生成
1208
署名の受信
1210
署名の送信
1209
三者署名付き契約情報の生成
1211

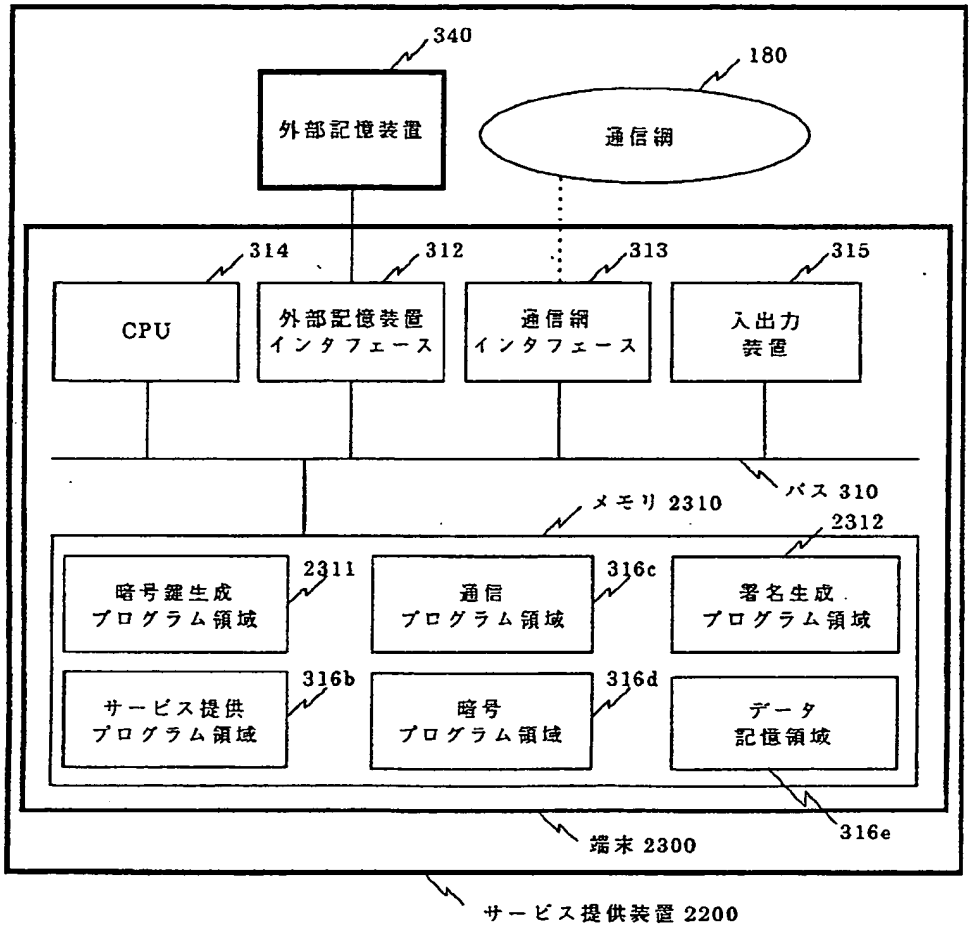
【図２４】


証明書 155
2223
認証機関 170
2220
証明書 153
2221
公開鍵 150
証明書 154
サービス提供装置 2200
フロッピーディスク 2220
三者署名付き契約情報 163
サービス提供者 100
163
160
163
契約情報 160
通信網 180
公開鍵 151
公開鍵 152
サービス享受者 110
サービス享受者 111
一者署名付き契約情報 161
一者署名付き契約情報 162
フロッピーディスク 2221
フロッピーディスク 2222
サービス享受装置 2210
サービス享受装置 2211

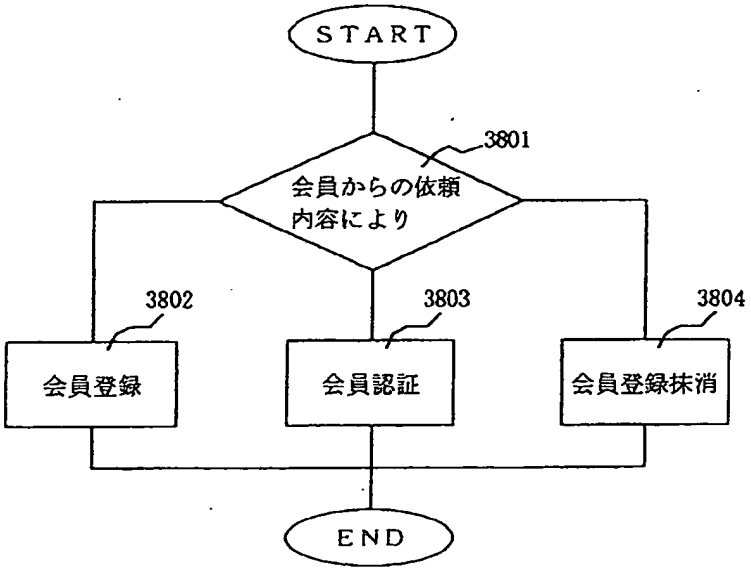
【図２７】


暗号化秘密鍵
2500
暗号化公開鍵
2503
ユーザID
2501
暗号化自証明書
2504
パスワード
チェック用データ
2502
認証機関証明書
2505
フロッピー
ディスク番号
2506
フロッピーディスク 2220

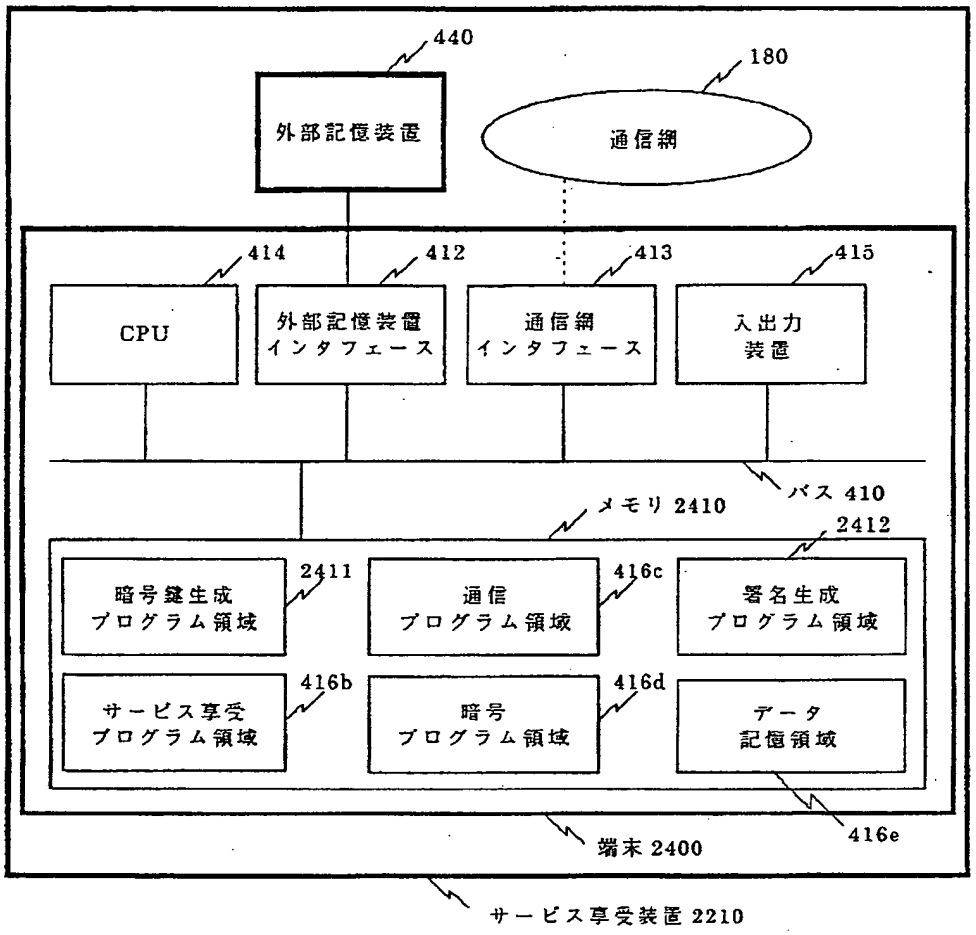
【図25】


340
外部記憶装置
180
通信網
314
CPU
312
外部記憶装置
インタフェース
313
通信網
インタフェース
315
入出力
装置
バス 310
メモリ 2310
2312
暗号鍵生成
プログラム領域
2311
通信
プログラム領域
316c
署名生成
プログラム領域
サービス提供
プログラム領域
316b
暗号
プログラム領域
316d
データ
記憶領域
316e
端末 2300
サービス提供装置 2200

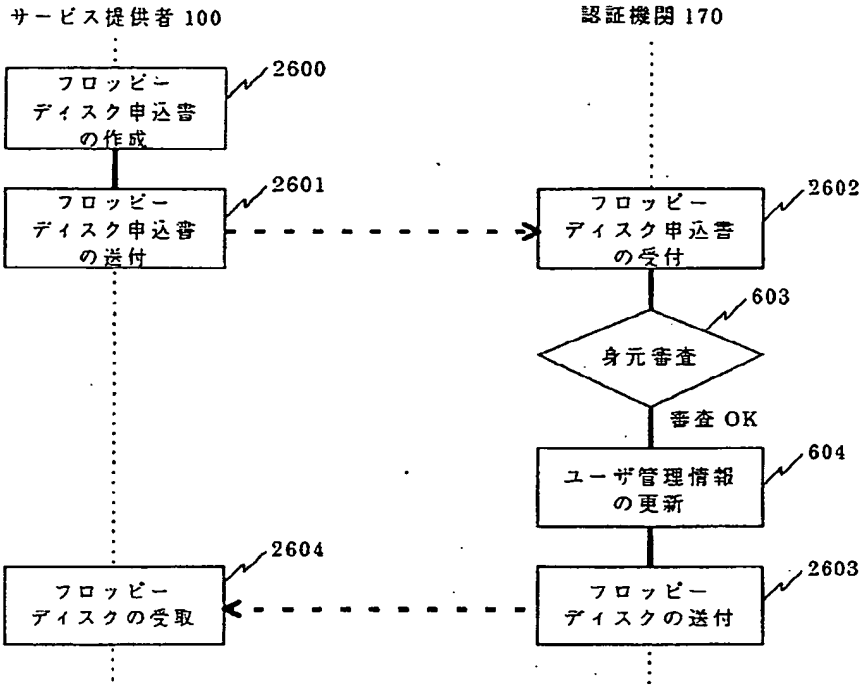
【図38】


START
3801
会員からの依頼
内容により
3802
会員登録
3803
会員認証
3804
会員登録抹消
END

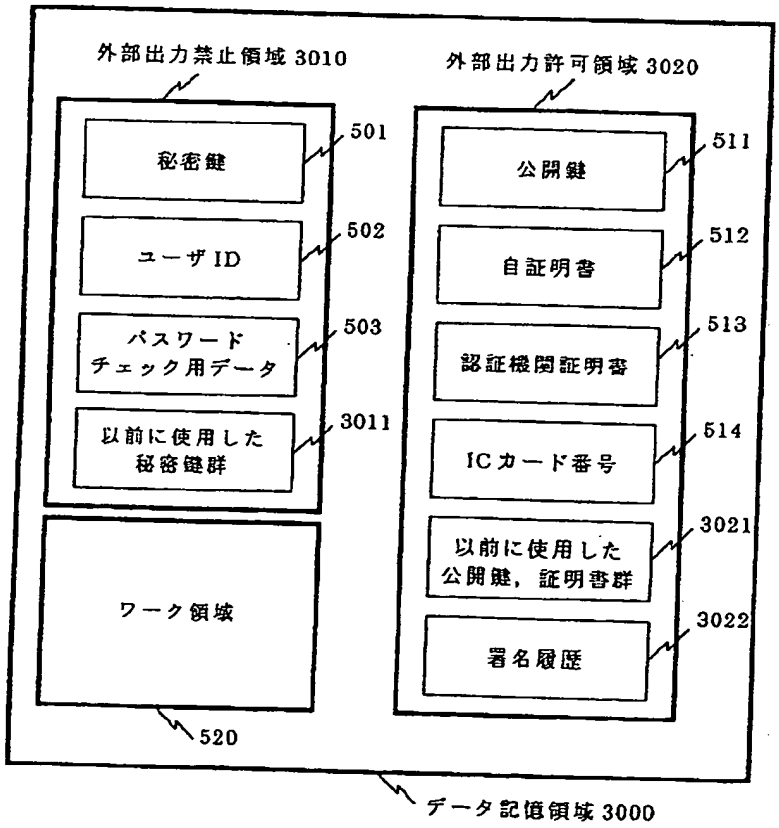
【図26】


440
外部記憶装置
180
通信網
414
CPU
412
外部記憶装置
インタフェース
413
通信網
インタフェース
415
入出力
装置
バス 410
メモリ 2410
2412
2411
暗号鍵生成
プログラム領域
416c
通信
プログラム領域
署名生成
プログラム領域
416b
サービス享受
プログラム領域
416d
暗号
プログラム領域
データ
記憶領域
416e
端末 2400
サービス享受装置 2210

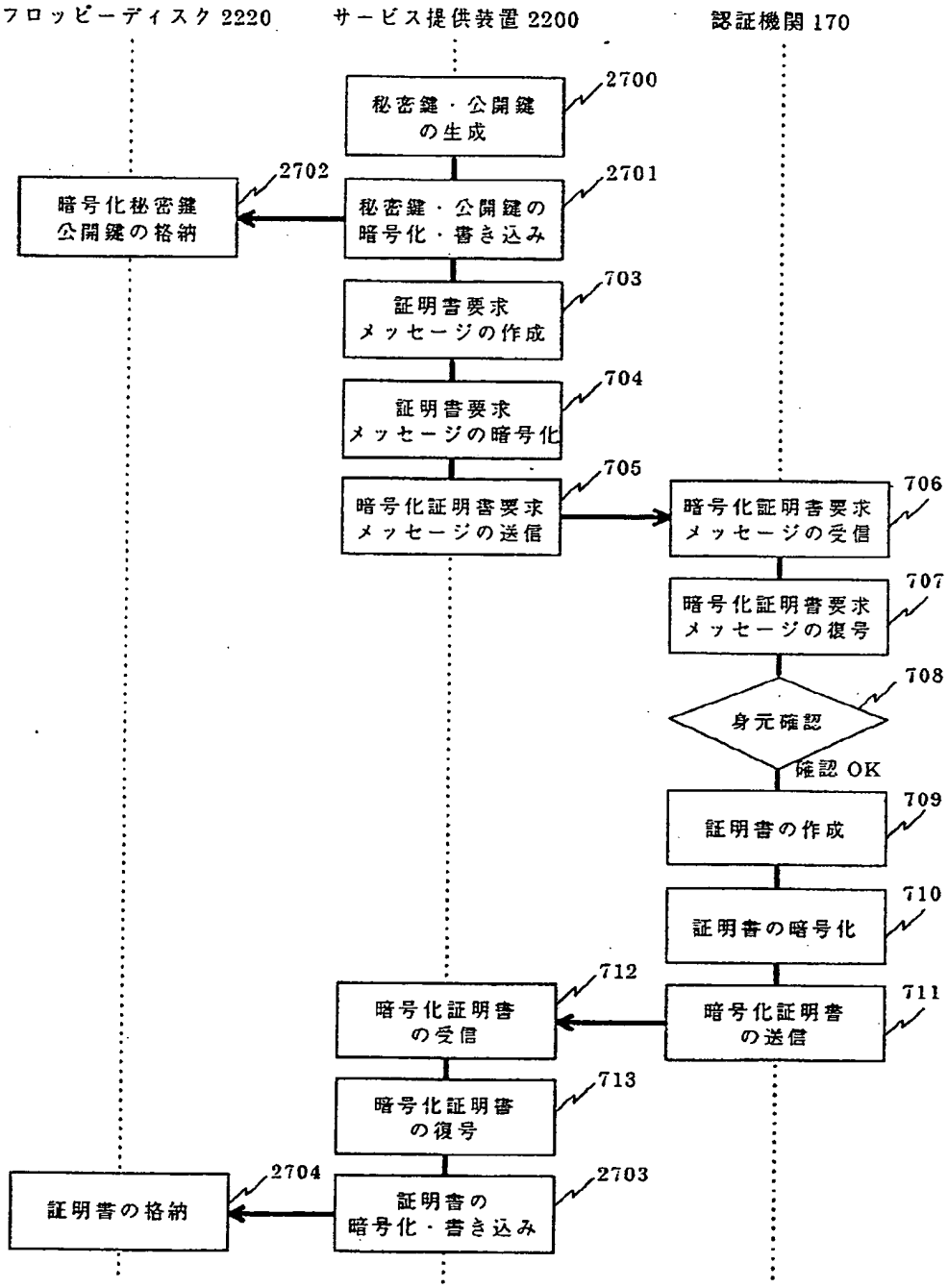
【図28】


サービス提供者 100
認証機関 170
フロッピーディスク申込書の作成
2600
フロッピーディスク申込書の送付
2601
フロッピーディスク申込書の受付
2602
603
身元審査
審査 OK
ユーザ管理情報の更新
604
フロッピーディスクの受取
2604
フロッピーディスクの送付
2603

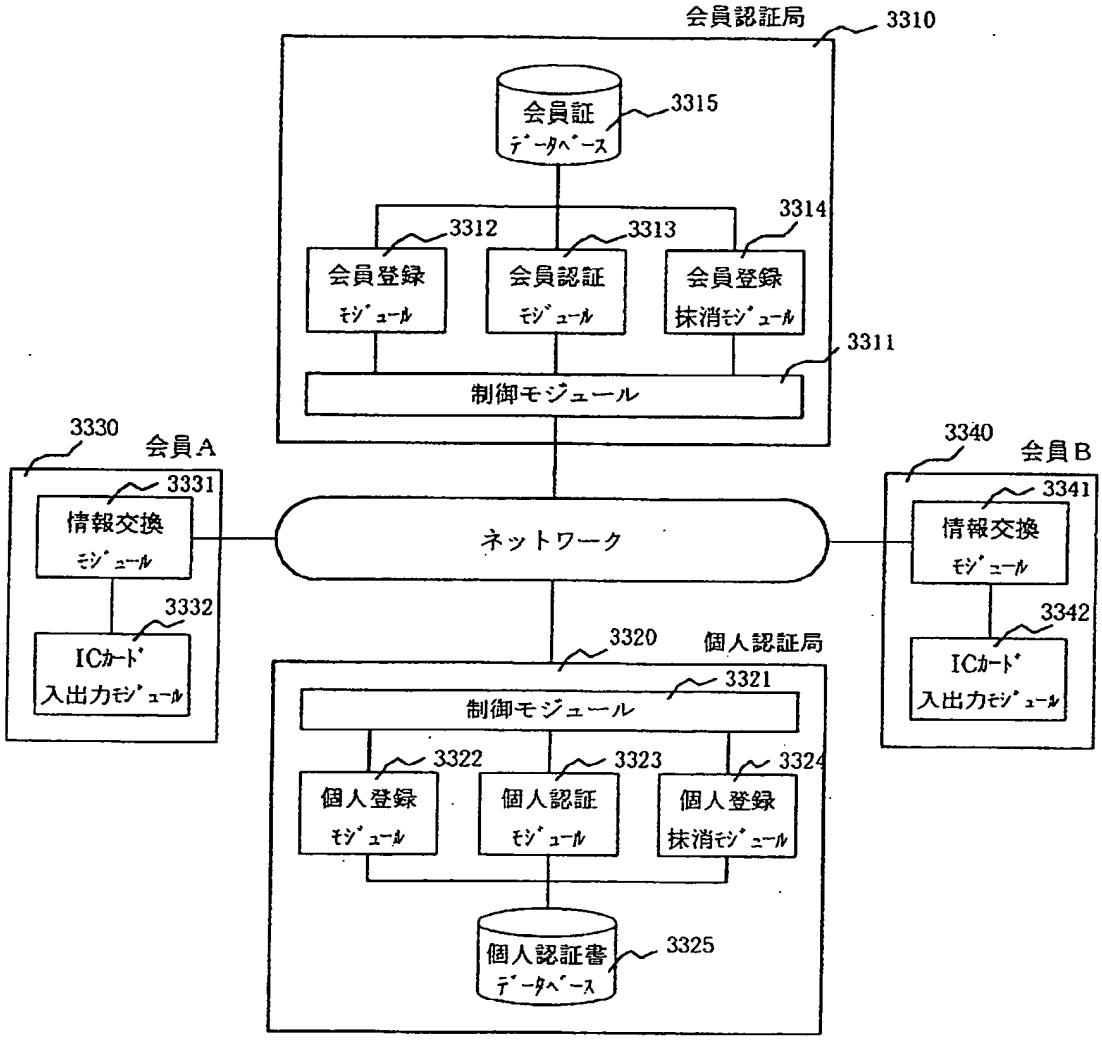
【図32】


外部出力禁止領域 3010
外部出力許可領域 3020
秘密鍵
501
ユーザ ID
502
パスワードチェック用データ
503
以前に使用した秘密鍵群
3011
ワーク領域
520
公開鍵
511
自証明書
512
認証機関証明書
513
IC カード番号
514
以前に使用した公開鍵，証明書群
3021
署名履歴
3022
データ記憶領域 3000

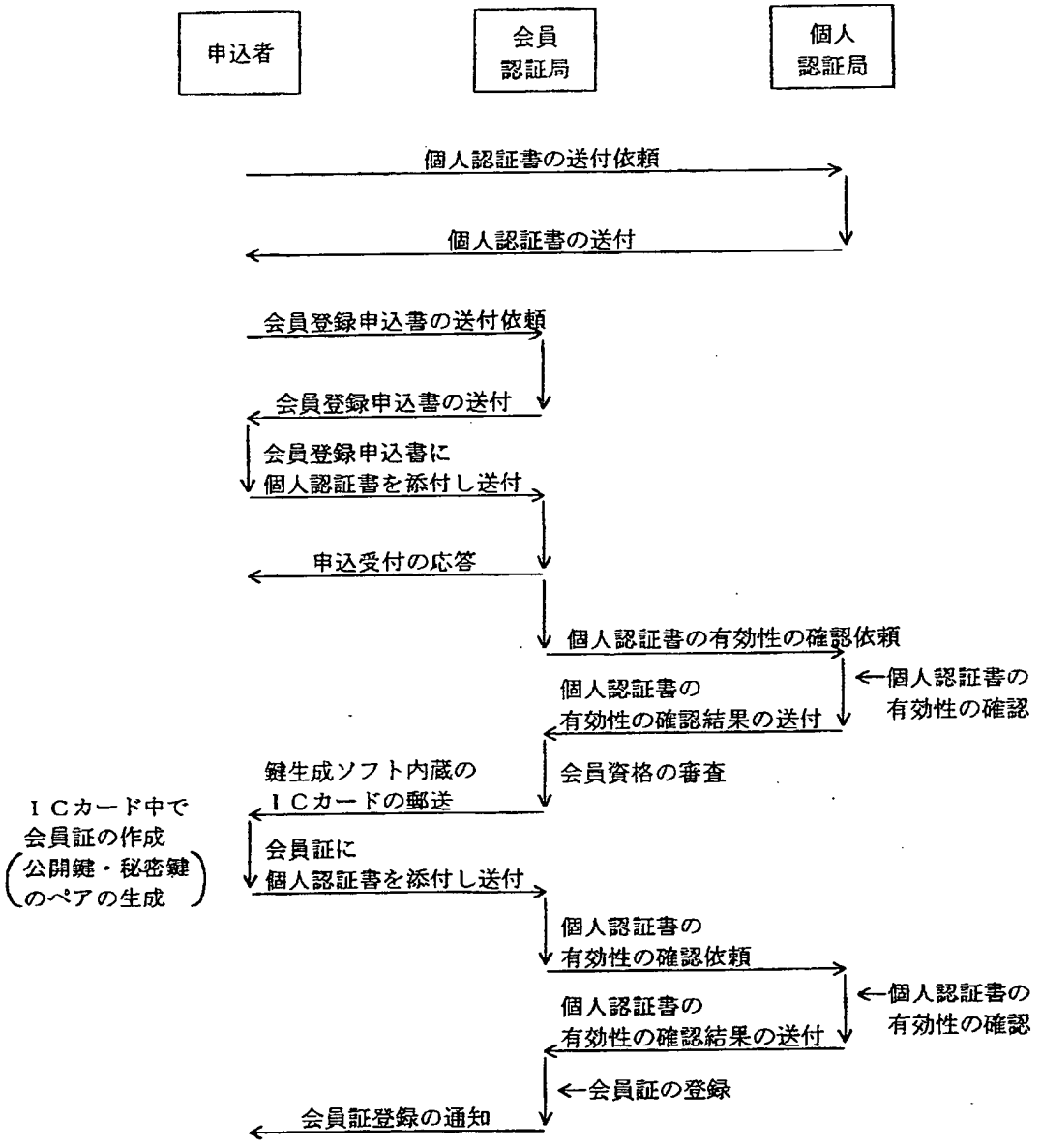
【図29】


フロッピーディスク 2220
サービス提供装置 2200
認証機関 170
秘密鍵・公開鍵の生成
2700
暗号化秘密鍵公開鍵の格納
2702
秘密鍵・公開鍵の暗号化・書き込み
2701
証明書要求メッセージの作成
703
証明書要求メッセージの暗号化
704
暗号化証明書要求メッセージの送信
705
暗号化証明書要求メッセージの受信
706
暗号化証明書要求メッセージの復号
707
身元確認
708
確認 OK
証明書の作成
709
証明書の暗号化
710
暗号化証明書の送信
711
暗号化証明書の受信
712
暗号化証明書の復号
713
証明書の格納
2704
証明書の暗号化・書き込み
2703

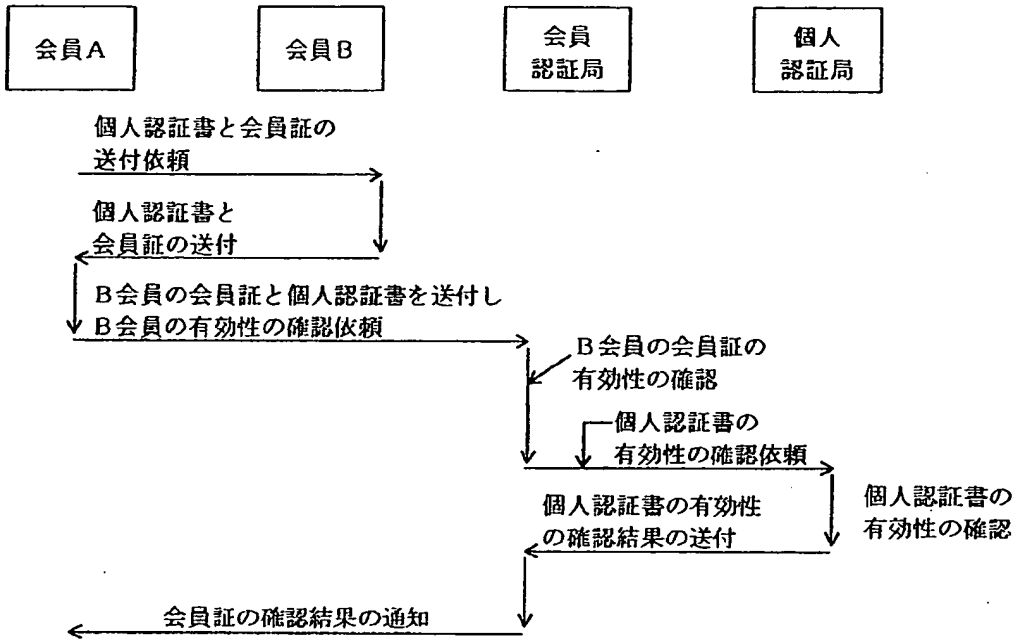
【図33】


会員認証局
3310
会員証
データベース
3315
3312
3313
3314
会員登録
モジュール
会員認証
モジュール
会員登録
抹消モジュール
3311
制御モジュール
3330
会員A
3331
情報交換
モジュール
3332
ICカード
入出力モジュール
ネットワーク
3340
会員B
3341
情報交換
モジュール
3342
ICカード
入出力モジュール
3320
個人認証局
3321
制御モジュール
3322
3323
3324
個人登録
モジュール
個人認証
モジュール
個人登録
抹消モジュール
個人認証書
データベース
3325

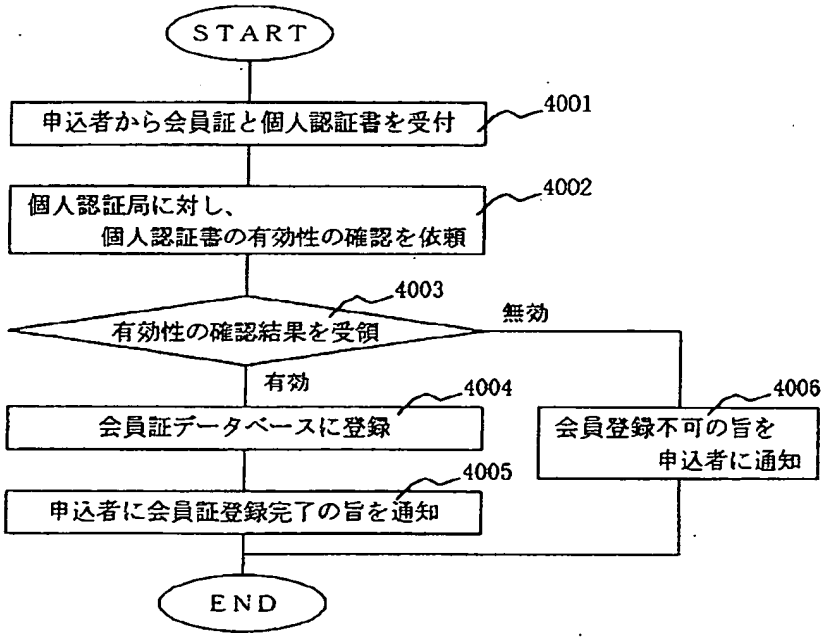
【図３５】


申込者
会員認証局
個人認証局
個人認証書の送付依頼
個人認証書の送付
会員登録申込書の送付依頼
会員登録申込書の送付
会員登録申込書に
個人認証書を添付し送付
申込受付の応答
個人認証書の有効性の確認依頼
←個人認証書の有効性の確認
個人認証書の
有効性の確認結果の送付
鍵生成ソフト内蔵の
ＩＣカードの郵送
会員資格の審査
ＩＣカード中で
会員証の作成
(公開鍵・秘密鍵
のペアの生成)
会員証に
個人認証書を添付し送付
個人認証書の
有効性の確認依頼
←個人認証書の有効性の確認
個人認証書の
有効性の確認結果の送付
←会員証の登録
会員証登録の通知

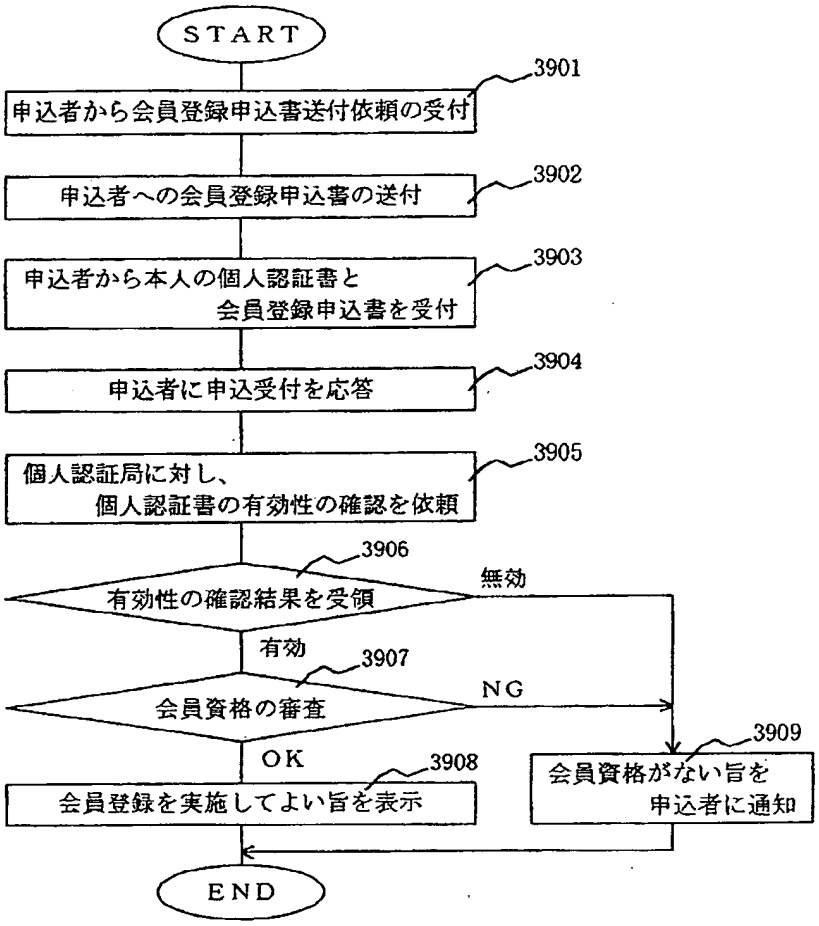
【図３７】


会員A
会員B
会員
認証局
個人
認証局
個人認証書と会員証の
送付依頼
個人認証書と
会員証の送付
B会員の会員証と個人認証書を送付し
B会員の有効性の確認依頼
B会員の会員証の
有効性の確認
個人認証書の
有効性の確認依頼
個人認証書の有効性
の確認結果の送付
個人認証書の
有効性の確認
会員証の確認結果の通知

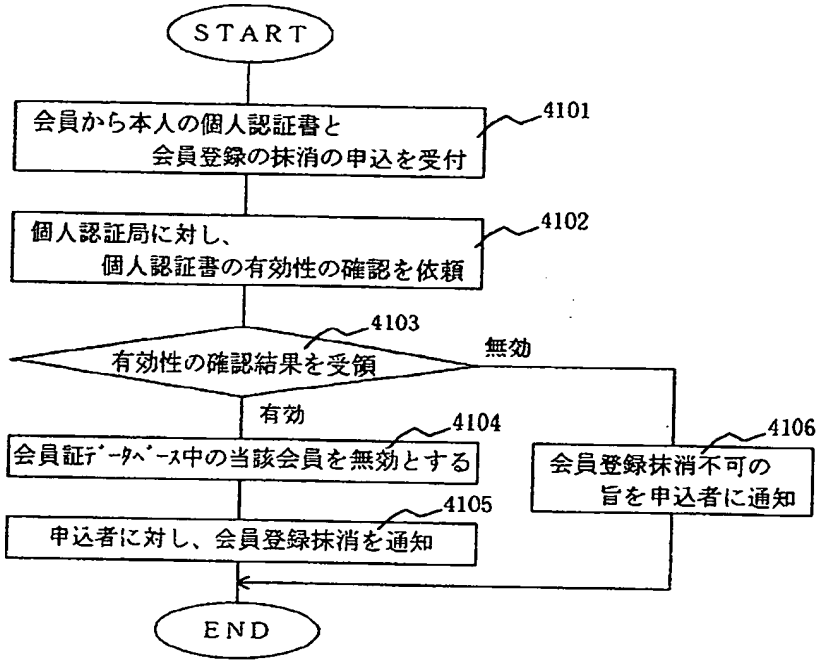
【図４０】


START
申込者から会員証と個人認証書を受付
4001
個人認証局に対し、
個人認証書の有効性の確認を依頼
4002
4003
有効性の確認結果を受領
無効
有効
4004
会員証データベースに登録
4006
会員登録不可の旨を
申込者に通知
4005
申込者に会員証登録完了の旨を通知
END

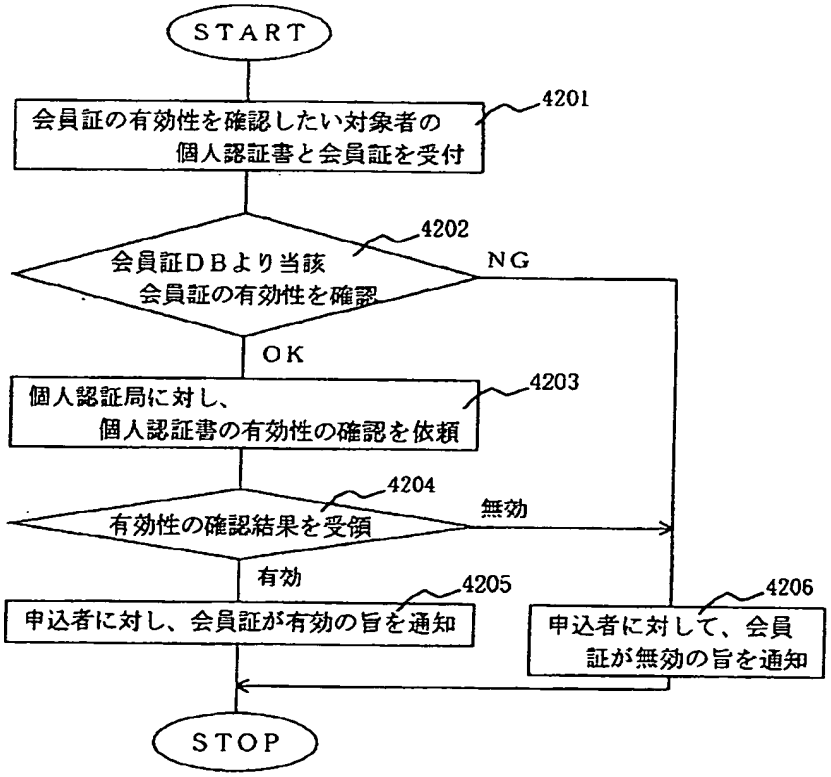
【図３９】


START
3901
申込者から会員登録申込書送付依頼の受付
3902
申込者への会員登録申込書の送付
3903
申込者から本人の個人認証書と
会員登録申込書を受付
3904
申込者に申込受付を応答
3905
個人認証局に対し、
個人認証書の有効性の確認を依頼
3906
有効性の確認結果を受領
無効
有効
3907
会員資格の審査
NG
OK
3908
会員登録を実施してよい旨を表示
3909
会員資格がない旨を
申込者に通知
END

【図41】

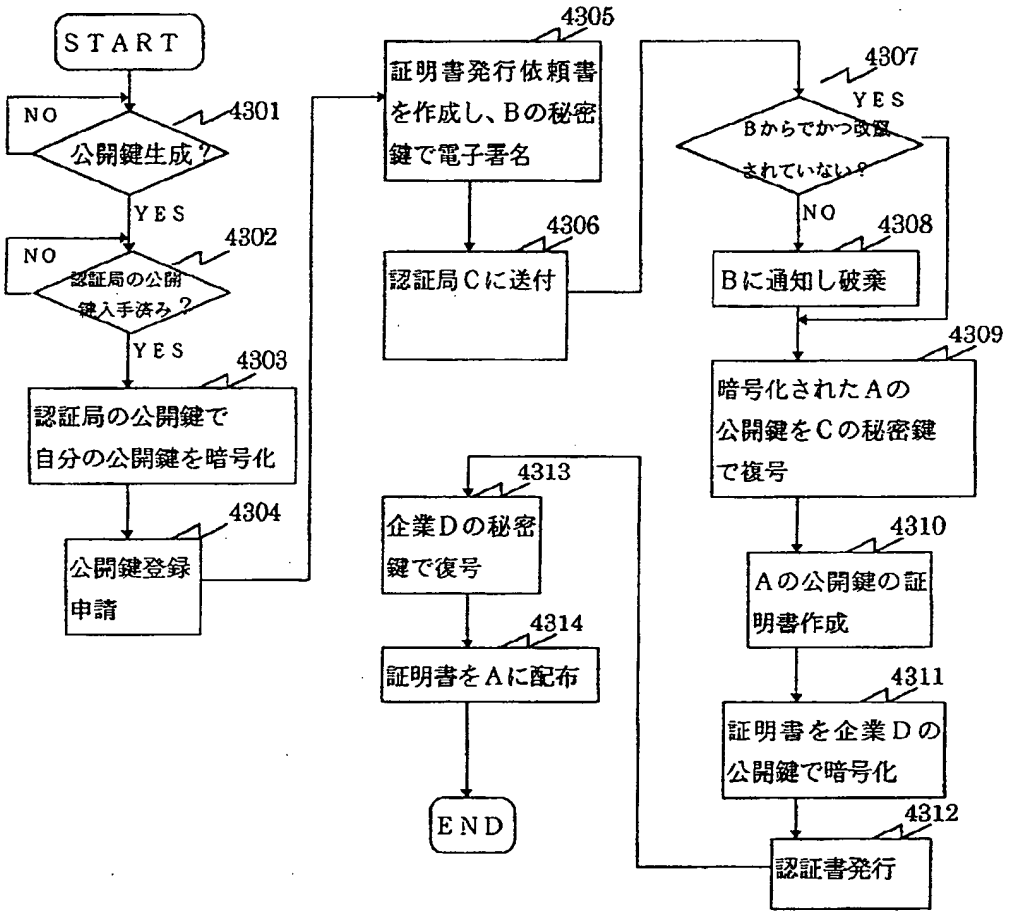

START
会員から本人の個人認証書と
会員登録の抹消の申込を受付
4101
個人認証局に対し、
個人認証書の有効性の確認を依頼
4102
有効性の確認結果を受領
4103
無効
有効
会員証ﾃﾞｰﾀﾍﾞｰｽ中の当該会員を無効とする
4104
会員登録抹消不可の
旨を申込者に通知
4106
申込者に対し、会員登録抹消を通知
4105
END

【図42】


START
会員証の有効性を確認したい対象者の
個人認証書と会員証を受付
4201
会員証DBより当該
会員証の有効性を確認
4202
NG
OK
個人認証局に対し、
個人認証書の有効性の確認を依頼
4203
有効性の確認結果を受領
4204
無効
有効
申込者に対し、会員証が有効の旨を通知
4205
申込者に対して、会員
証が無効の旨を通知
4206
STOP

【図４３】

企業内認証における公開鍵登録の処理フロー




---

フロントページの続き

(72)発明者　高橋　美和
神奈川県川崎市幸区鹿島田890番地　株式会社日立製作所ビジネスシステム開発センタ内

(72)発明者　光永　聖
神奈川県川崎市幸区鹿島田890番地　株式会社日立製作所情報システム事業部内

(72)発明者　森山　将治
神奈川県川崎市幸区鹿島田890番地　株式会社日立製作所情報システム事業部内